Wireless LAN Mobility System

Wireless LAN Switch and Controller Command Reference

WX4400	3CRWX440095A
WX1200	3CRWX120695A
WXR100	3CRWXR10095A

http://www.3com.com/

Part No. 10015086
Published April 2006

Downloaded from www.Manualslib.com manuals search engine

3Com Corporation
350 Campus Drive
Marlborough, MA USA
01752-3064

Copyright © 2006, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com is a registered trademark of 3Com Corporation. The 3Com logo is a trademark of 3Com Corporation.

Mobility Domain, Mobility Point, Mobility Profile, Mobility System, Mobility System Software, MP, MSS, and SentrySweep are trademarks of Trapeze Networks, Inc.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, Windows XP, and Windows NT are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

Downloaded from www.Manualslib.com manuals search engine

CONTENTS

ABOUT THIS GUIDE

Conventions 19
Documentation 20
Documentation Comments 21

1 USING THE COMMAND-LINE INTERFACE

Overview 23
CLI Conventions 24
- Command Prompts 24
- Syntax Notation 24
- Text Entry Conventions and Allowed Characters 25
- MAC Address Notation 25
- IP Address and Mask Notation 26
- User Globs, MAC Address Globs, and VLAN Globs 26
- Port Lists 28
- Virtual LAN Identification 29

Command-Line Editing 29
- Keyboard Shortcuts 29
- History Buffer 30
- Tabs 30
- Single-Asterisk (*) Wildcard Character 30
- Double-Asterisk (**) Wildcard Characters 30

Using CLI Help 31
Understanding Command Descriptions 32

2 ACCESS COMMANDS

Commands by Usage 33
disable 33
enable 34
quit 34
set enablepass 35

Downloaded from www.Manualslib.com manuals search engine

3 SYSTEM SERVICE COMMANDS

Commands by Usage 37
clear banner motd 38
clear history 39
clear prompt 39
clear system 40
display banner motd 41
display base-information 41
display license 42
display load 43
display system 43
help 46
history 47
quickstart 48
set auto-config 48
set banner motd 51
set confirm 52
set length 53
set license 53
set prompt 54
set system contact 55
set system countrycode 56
set system idle-timeout 58
set system ip-address 59
set system location 59
set system name 60

4 PORT COMMANDS

Commands by Usage 63
clear dap 64
clear port counters 65
clear port-group 65
clear port media-type 66
clear port name 66
clear port preference 67
clear port type 68
display port counters 69

Downloaded from www.Manualslib.com manuals search engine

display port-group 70
display port poe 71
display port preference 72
display port status 73
display port media-type 75
monitor port counters 76
reset port 81
set dap 81
set port 83
set port-group 84
set port media-type 85
set port name 86
set port negotiation 86
set port poe 87
set port preference 88
set port speed 89
set port trap 90
set port type ap 91
set port type wired-auth 94

5 VLAN COMMANDS

Commands by usage 97
clear fdb 98
clear security 12-restrict 99
clear security 12-restrict counters 100
clear vlan 101
display fdb 102
display fdb agingtime 104
display fdb count 105
display roaming station 106
display roaming vlan 108
display security 12-restrict 109
display tunnel 110
display vlan config 111
set fdb 113
set fdb agingtime 114
set security l2-restrict 114

Downloaded from www.Manualslib.com manuals search engine

set vlan name 116
set vlan port 117
set vlan tunnel-affinity 118

6 QUALITY OF SERVICE COMMANDS

Commands by Usage 119
clear qos 120
set qos cos-to-dscp-map 121
set qos dscp-to-cos-map 122
display qos 123
display qos dscp-table 124

7 IP SERVICES COMMANDS

Commands by Usage 125
clear interface 127
clear ip alias 128
clear ip dns domain 129
clear ip dns server 129
clear ip route 130
clear ip telnet 131
clear ntp server 131
clear ntp update-interval 132
clear snmp community 133
clear snmp notify profile 133
clear snmp notify target 134
clear snmp usm 134
clear summertime 135
clear system ip-address 136
clear timezone 136
display arp 137
display dhcp-client 138
display dhcp-server 140
display interface 142
display ip alias 143
display ip dns 144
display ip https 145
display ip route 146

Downloaded from www.Manualslib.com manuals search engine

display ip telnet 148
display ntp 149
display snmp community 151
display snmp counters 152
display snmp notify profile 152
display snmp notify target 152
display snmp status 153
display snmp usm 154
display summertime 154
display timedate 155
display timezone 155
ping 156
set arp 158
set arp agingtime 159
set interface 160
set interface dhcp-client 161
set interface dhcp-server 162
set interface status 163
set ip alias 164
set ip dns 164
set ip dns domain 165
set ip dns server 166
set ip https server 167
set ip route 167
set ip snmp server 169
set ip ssh 170
set ip ssh server 171
set ip telnet 171
set ip telnet server 172
set ntp 173
set ntp server 174
set ntp update-interval 175
set snmp community 175
set snmp notify profile 177
set snmp notify target 181
SNMPv3 with Informs 181
SNMPv3 with Traps 183
SNMPv2c with Informs 183

Downloaded from www.Manualslib.com manuals search engine

SNMPv2c with Traps 184
SNMPv1 with Traps 184
set snmp protocol 186
set snmp security 187
set snmp usm 188
set summertime 191
set system ip-address 192
set timedate 193
set timezone 194
telnet 195
traceroute 197

8 AAA COMMANDS

Commands by Usage 201
clear accounting 203
clear authentication admin 204
clear authentication console 205
clear authentication dot1x 206
clear authentication last-resort 207
clear authentication mac 208
clear authentication proxy 209
clear authentication web 209
clear location policy 210
clear mac-user 211
clear mac-user attr 212
clear mac-user group 212
clear mac-usergroup 213
clear mac-usergroup attr 214
clear mobility-profile 215
clear user 215
clear user attr 216
clear user group 217
clear usergroup 217
clear usergroup attr 218
display aaa 219
display accounting statistics 222
display location policy 224

Downloaded from www.Manualslib.com manuals search engine

display mobility-profile 224
set accounting {admin | console} 225
set accounting {dot1x | mac | web | last-resort} 227
set authentication admin 229
set authentication console 231
set authentication dot1x 233
set authentication last-resort 236
set authentication mac 239
set authentication proxy 241
set authentication web 242
set location policy 244
set mac-user 248
set mac-user attr 249
set mac-usergroup attr 254
set mobility-profile 255
set mobility-profile mode 257
set user 258
set user attr 259
set user group 260
set usergroup 261
set web-portal 262

9 MOBILITY DOMAIN COMMANDS
Commands by Usage 265
clear mobility-domain 266
clear mobility-domain member 266
display mobility-domain config 267
display mobility-domain status 267
set mobility-domain member 269
set mobility-domain mode member seed-ip 270
set mobility-domain mode seed domain-name 271

10 NETWORK DOMAIN COMMANDS
Network Domain Commands by Usage 273
clear network-domain 274
clear network-domain mode 275
clear network-domain peer 276

Downloaded from www.Manualslib.com manuals search engine

clear network-domain seed-ip 277
display network-domain 278
set network-domain mode member seed-ip 280
set network-domain peer 281
set network-domain mode seed domain-name 282

11 MANAGED ACCESS POINT COMMANDS

MAP Access Point Commands by Usage 283
clear {ap | dap} radio 286
clear radio-profile 288
clear service-profile 289
display {ap | dap} config 290
display {ap | dap} counters 294
display {ap | dap} qos-stats 300
display {ap | dap} etherstats 301
display {ap | dap} group 303
display {ap | dap} status 304
display auto-tune attributes 309
display auto-tune neighbors 311
display dap connection 313
display dap global 314
display dap unconfigured 316
display radio-profile 317
display service-profile 321
reset {ap | dap} 324
set dap auto 325
set dap auto radiotype 326
set dap auto mode 327
set {ap | dap} bias 328
set {ap | dap} blink 330
set dap fingerprint 331
set {ap | dap} group 332
set {ap | dap} name 333
set {ap | dap} radio antennatype 334
set {ap | dap} radio auto-tune max-power 335
set {ap | dap} radio auto-tune max-retransmissions 337
set {ap | dap} radio channel 339

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} radio auto-tune min-client-rate 340
set {ap | dap} radio mode 341
set {ap | dap} radio radio-profile 343
set {ap | dap} radio tx-power 344
set dap security 345
set {ap | dap} upgrade-firmware 346
set radio-profile 11g-only 347
set radio-profile active-scan 348
set radio-profile auto-tune channel-config 349
set radio-profile auto-tune channel-holddown 350
set radio-profile auto-tune channel-interval 351
set radio-profile auto-tune power-backoff- timer 352
set radio-profile auto-tune power-config 353
set radio-profile auto-tune power-interval 354
set radio-profile beacon-interval 355
set radio-profile countermeasures 355
set radio-profile dtim-interval 357
set radio-profile frag-threshold 358
set radio-profile long-retry 359
set radio-profile max-rx-lifetime 360
set radio-profile max-tx-lifetime 361
set radio-profile mode 362
set radio-profile preamble-length 364
set radio-profile rts-threshold 365
set radio-profile service-profile 366
set radio-profile short-retry 369
set radio-profile wmm 370
set service-profile attr 371
set service-profile auth-dot1x 373
set service-profile auth-fallthru 374
set service-profile auth-psk 375
set service-profile beacon 376
set service-profile cipher-ccmp 377
set service-profile cipher-tkip 378
set service-profile cipher-wep104 379
set service-profile cipher-wep40 380
set service-profile psk-phrase 381
set service-profile psk-raw 382

Downloaded from www.Manualslib.com manuals search engine

set service-profile rsn-ie 383
set service-profile shared-key-auth 384
set service-profile ssid-name 384
set service-profile ssid-type 385
set service-profile tkip-mc-time 386
set service-profile web-portal-form 387
set service-profile wep active-multicast-index 388
set service-profile wep active-unicast-index 389
set service-profile wep key-index 390
set service-profile wpa-ie 391

12 STP COMMANDS

STP Commands by Usage 393
clear spantree portcost 394
clear spantree portpri 395
clear spantree portvlancost 395
clear spantree portvlanpri 396
clear spantree statistics 397
display spantree 398
display spantree backbonefast 400
display spantree blockedports 401
display spantree portfast 402
display spantree portvlancost 403
display spantree statistics 403
display spantree uplinkfast 409
set spantree 410
set spantree backbonefast 411
set spantree fwddelay 412
set spantree hello 412
set spantree maxage 413
set spantree portcost 414
set spantree portfast 415
set spantree portpri 416
set spantree portvlancost 417
set spantree portvlanpri 418
set spantree priority 419
set spantree uplinkfast 419

Downloaded from www.Manualslib.com manuals search engine

13 IGMP SNOOPING COMMANDS

Commands by usage 421
clear igmp statistics 422
display igmp 422
display igmp mrouter 426
display igmp querier 427
display igmp receiver-table 429
display igmp statistics 431
set igmp 433
set igmp lmqi 434
set igmp mrouter 435
set igmp mrsol 436
set igmp mrsol mrsi 436
set igmp oqi 437
set igmp proxy-report 438
set igmp qi 439
set igmp qri 440
set igmp querier 441
set igmp receiver 441
set igmp rv 442

14 SECURITY ACL COMMANDS

Security ACL Commands by Usage 445
clear security acl 446
clear security acl map 447
commit security acl 449
display security acl 450
display security acl hits 451
display security acl info 452
display security acl map 453
display security acl resource-usage 454
rollback security acl 458
set security acl 459
set security acl map 464
set security acl hit-sample-rate 466

Downloaded from www.Manualslib.com manuals search engine

15 CRYPTOGRAPHY COMMANDS

Commands by Usage 469
crypto ca-certificate 470
crypto certificate 471
crypto generate key 473
crypto generate request 474
crypto generate self-signed 476
crypto otp 478
crypto pkcs12 479
display crypto ca-certificate 481
display crypto certificate 482
display crypto key ssh 483

16 RADIUS AND SERVER GROUP COMMANDS

Commands by Usage 485
clear radius 486
clear radius client system-ip 487
clear radius proxy client 488
clear radius proxy port 488
clear radius server 489
clear server group 489
set radius 490
set radius client system-ip 491
set radius proxy client 492
set radius proxy port 493
set radius server 494
set server group 496
set server group load-balance 497

17 802.1X MANAGEMENT COMMANDS

Commands by Usage 499
clear dot1x bonded-period 500
clear dot1x max-req 501
clear dot1x port-control 501
clear dot1x quiet-period 502
clear dot1x reauth-max 503

Downloaded from www.Manualslib.com manuals search engine

clear dot1x reauth-period 503
clear dot1x timeout auth-server 504
clear dot1x timeout supplicant 504
clear dot1x tx-period 505
display dot1x 505
set dot1x authcontrol 508
set dot1x bonded-period 509
set dot1x key-tx 510
set dot1x max-req 511
set dot1x port-control 512
set dot1x quiet-period 513
set dot1x reauth 513
set dot1x reauth-max 514
set dot1x reauth-period 515
set dot1x timeout auth-server 515
set dot1x timeout supplicant 516
set dot1x tx-period 516
set dot1x wep-rekey 517
set dot1x wep-rekey-period 518

18 SESSION MANAGEMENT COMMANDS
Commands by Usage 519
clear sessions 519
clear sessions network 521
display sessions 522
display sessions network 525

19 RF DETECTION COMMANDS
Commands by Usage 533
clear rfdetect attack-list 534
clear rfdetect black-list 535
clear rfdetect ignore 535
clear rfdetect ssid-list 536
clear rfdetect vendor-list 537
display rfdetect attack-list 537
display rfdetect black-list 538
display rfdetect clients 539

Downloaded from www.Manualslib.com manuals search engine

display rfdetect countermeasures 541
display rfdetect counters 542
display rfdetect data 544
display rfdetect ignore 546
display rfdetect mobility-domain 546
display rfdetect ssid-list 550
display rfdetect vendor-list 551
display rfdetect visible 552
set rfdetect active-scan 554
set rfdetect attack-list 554
set rfdetect black-list 555
set rf detect countermeasures 556
set rfdetect countermeasures mac 557
set rfdetect ignore 558
set rfdetect log 559
set rfdetect signature 560
set rfdetect ssid-list 560
set rfdetect vendor-list 561

20 FILE MANAGEMENT COMMANDS

Commands by Usage 563
backup 564
clear boot backup-configuration 566
clear boot config 566
copy 567
delete 569
dir 570
display boot 573
display config 574
display version 576
load config 578
md5 580
mkdir 580
reset system 582
restore 583
rmdir 584
save config 584

Downloaded from www.Manualslib.com manuals search engine

set boot backup-configuration 585
set boot configuration-file 586
set boot partition 587

21 TRACE COMMANDS

Commands by Usage 589
clear log trace 590
clear trace 590
display trace 591
save trace 592
set trace authentication 592
set trace authorization 593
set trace dot1x 594
set trace sm 595

22 SNOOP COMMANDS

Commands by Usage 597
clear snoop 598
clear snoop map 598
set snoop 599
set snoop map 602
set snoop mode 603
display snoop 604
display snoop info 604
display snoop map 605
display snoop stats 606

23 SYSTEM LOG COMMANDS

Commands by Usage 609
clear log 609
display log buffer 610
display log config 612
display log trace 613
set log 614
set log mark 616

Downloaded from www.Manualslib.com manuals search engine

24 BOOT PROMPT COMMANDS

Boot Prompt Commands by Usage 619
autoboot 620
boot 621
change 623
create 624
delete 625
dhcp 626
diag 627
dir 627
display 628
fver 630
help 631
ls 632
next 633
reset 634
test 635
version 636

A OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product 637
Purchase Value-Added Services 637
Troubleshoot Online 638
Access Software Downloads 638
Telephone Technical Support and Repair 638
Contact Us 639

INDEX

Downloaded from www.Manualslib.com manuals search engine

ABOUT THIS GUIDE

This command reference explains Mobility System Software (MSS™) command line interface (CLI) that you enter on a 3Com WXR100 or WX1200 Wireless Switch or WX4400 Wireless LAN Controller to configure and manage the Mobility System™ wireless LAN (WLAN).

Read this reference if you are a network administrator responsible for managing WXR100, WX1200 or WX4400 wireless switches and their Managed Access Points (MAPs) in a network.

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

http://www.3com.com/

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device

Downloaded from www.Manualslib.com manuals search engine

This manual uses the following text and syntax conventions:

Table 2 Text Conventions

Convention	Description
`Monospace text`	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
Italic text	Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.
[ ] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
| (vertical bar)	Separates mutually exclusive options in command syntax.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ▪ Emphasize a point. ▪ Denote a new term at the place where it is defined in the text. ▪ Highlight an example string, such as a username or SSID.

Documentation

The MSS documentation set includes the following documents.

- *Wireless LAN Switch Manager (3WXM) Release Notes*

  These notes provide information about the system software release, including new features and bug fixes.

- *Wireless LAN Switch and Controller Release Notes*

  These notes provide information about the system software release, including new features and bug fixes.

- *Wireless LAN Switch and Controller Quick Start Guide*

  This guide provides instructions for performing basic setup of secure (802.1X) and guest (WebAAA™) access, for configuring a Mobility Domain for roaming, and for accessing a sample network plan in 3WXM for advanced configuration and management.

Downloaded from www.Manualslib.com manuals search engine

- *Wireless LAN Switch Manager Reference Manual*

  This manual shows you how to plan, configure, deploy, and manage a Mobility System wireless LAN (WLAN) using the 3Com Wireless LAN Switch Manager (3WXM).

- *Wireless LAN Switch Manager User's Guide*

  This manual shows you how to plan, configure, deploy, and manage the entire WLAN with the 3WXM tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy 3Com equipment to provide those services, and how to optimize and manage your WLAN.

- *Wireless LAN Switch and Controller Hardware Installation Guide*

  This guide provides instructions and specifications for installing a WX wireless switch in a Mobility System WLAN.

- *Wireless LAN Switch and Controller Configuration Guide*

  This guide provides instructions for configuring and managing the system through the Mobility System Software (MSS) CLI.

- *Wireless LAN Switch and Controller Command Reference*

  This reference provides syntax information for all MSS commands supported on WX switches.

Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when contacting us:

- *Document title*
- *Document part number and revision (on the title page)*
- *Page number (if appropriate)*

Example:

- *Wireless LAN Switch and Controller Configuration Guide*
- *Part number 730-9502-0071, Revision B*
- *Page 25*

Downloaded from www.Manualslib.com manuals search engine

Please note that we can only respond to comments and questions about 3Com product documentation at this e-mail address. Questions related to Technical Support or sales should be directed in the first instance to your network supplier.

Downloaded from www.Manualslib.com manuals search engine

1 USING THE COMMAND-LINE INTERFACE

This chapter discusses the 3Com Wireless Switch Manager (3WXM) command-line interface (CLI). Described are:

- CLI conventions (see "CLI Conventions" on page 24)
- Editing on the command line (see "Command-Line Editing" on page 29)
- Using the CLI help feature (see "Using CLI Help" on page 31)
- Information about the command descriptions in this reference (see "Understanding Command Descriptions" on page 32)

Overview

Mobility System Software (MSS) operates a 3Com Mobility System wireless LAN (WLAN) consisting of 3Com Wireless Switch Manager (3WXM) software and 3Com Wireless LAN Switch or 3Com Wireless LAN Controller (WX switch) and 3Com Wireless LAN Managed Access Point (MAP) hardware. There is a command-line interface (CLI) on the WX switch that you can use to configure and manage the WX and its attached access points.

You configure the wireless LAN switches and access points primarily with **set, clear,** and **display** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **display** commands to show the current configuration and monitor the status of network operations.

The wireless LAN switches support two connection modes:

- Administrative access mode, which enables the network administrator to connect *to* the WX switch and configure the network
- Network access mode, which enables network users to connect *through* the WX switch to access the network

Downloaded from www.Manualslib.com manuals search engine

CLI Conventions

Be aware of the following MSS CLI conventions for command entry:

- "Command Prompts" on page 24
- "Syntax Notation" on page 24
- "Text Entry Conventions and Allowed Characters" on page 25
- "User Globs, MAC Address Globs, and VLAN Globs" on page 26
- "Port Lists" on page 28
- "Virtual LAN Identification" on page 29

Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The *mmmm* portion shows the wireless LAN switch model number (for example, *1200*).

```
WXmmmm>
```

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, MSS displays the following prompt:

```
WXmmmm#
```

For information about changing the CLI prompt on a wireless LAN switch, see "set prompt" on page 54.

Syntax Notation

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

  `set enablepass`

- Italics indicate a placeholder for a value. For example, you replace *vlan-id* in the following command with a virtual LAN (VLAN) ID:

  `clear interface` *`vlan-id`* **`ip`**

- Curly brackets (**{ }**) indicate a mandatory parameter, and square brackets (**[ ]**) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

  `clear fdb` {**`dynamic`** | **`port`** *`port-list`*} [**`vlan`** *`vlan-id`*]

Downloaded from www.Manualslib.com manuals search engine

- A vertical bar (**|**) separates mutually exclusive options within a list of possibilities. For example, you enter either **enable** or **disable**, not both, in the following command:

  set port {**enable** | **disable**} *port-list*

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

3Com recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names *red* and *RED*.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (" ").

In addition, the CLI does not support the use of international characters such as the accented *É* in DÉCOR.

MAC Address Notation

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes — for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (**-**) or colon (**:**) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MSS displays of MAC addresses include all leading zeros.
- In some specified commands, you can use the single-asterisk (*****) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see "MAC Address Globs" on page 27.)

Downloaded from www.Manualslib.com manuals search engine

IP Address and Mask Notation

MSS displays IP addresses in dotted decimal notation — for example, 192.168.1.111. MSS makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks — for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (**/**) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the wireless LAN switch filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any *0*s (zeros) in the mask, but does not check the bits that correspond to *1*s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

User Globs, MAC Address Globs, and VLAN Globs

Name "globbing" is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (******) wildcard characters with no delimiter characters match *all* usernames. The single-asterisk (*****) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the *at* (@) sign and the period (.).

Downloaded from www.Manualslib.com manuals search engine

Table 3 gives examples of user globs.

Table 3 User Globs

User Glob	User(s) Designated
jose@example.com	User *jose* at example.com
*@example.com	All users at example.com whose usernames do not contain periods — for example, jose@example.com and tamara@example.com, but *not* nin.wong@example.com, because nin.wong contains a period
*@marketing.example.com	All marketing users at example.com whose usernames do not contain periods
.@marketing.example.com	All marketing users at example.com whose usernames contain periods
*	All users with usernames that have no delimiters
EXAMPLE*	All users in the Windows Domain EXAMPLE with usernames that have no delimiters
EXAMPLE*.*	All users in the Windows Domain EXAMPLE whose usernames contain periods
**	All users

MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match *all* MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*
00:01:*
00:01:02:*
00:01:02:03:*
00:01:02:03:04:*
```

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

Downloaded from www.Manualslib.com manuals search engine

VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on an wireless LAN switch, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (******) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*****) wildcard. Valid VLAN glob delimiter characters are the *at* (@) sign and the period (.).

For example, the VLAN glob *bldg4.** matches *bldg4.security* and *bldg4.hr* and all other VLAN names with *bldg4.* at the beginning.

Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which MSS matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the **display aaa** or **display config** command. MSS checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Port Lists

The physical Ethernet ports on a WX switch can be set for connection to MAP access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on a WX switch are numbered 1 through 4 (for the 3Com Wireless LAN Controller WX4400) and 1 through 8 (for the 3Com Wireless Lan Switch WX1200). No port 0 exists on the WX switch. You can include a single port or multiple ports in a command that includes **port *port-list.*** Use one of the following formats for ***port-list***:

- A single port number. For example:

  ```
  WX1200# set port enable 6
  ```

- A comma-separated list of port numbers, with no spaces. For example:

  ```
  WX1200# display port poe 1,2,4
  ```

Downloaded from www.Manualslib.com manuals search engine

- A hyphen-separated range of port numbers, with no spaces. For example:

  ```
  WX1200# reset port 1-3
  ```

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

  ```
  WX1200# display port status 1-3,6
  ```

Virtual LAN Identification

The *names* of virtual LANs (VLANs), which are used in Mobility Domain™ communications, are set by you and can be changed. In contrast, VLAN ID *numbers*, which the wireless LAN uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI **set** and **display** commands use a VLAN's name or number to uniquely identify the VLAN within the WX.

Command-Line Editing

MSS editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following table lists the keyboard shortcuts for entering and editing CLI commands.

Table 4 Keyboard Shortcuts

Keyboard Shortcut(s)	Function
Ctrl+A	Jumps to the first character of the command line.
Ctrl+B or Left Arrow key	Moves the cursor back one character.
Ctrl+C	Escapes and terminates prompts and tasks.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Jumps to the end of the current command line.
Ctrl+F or Right Arrow key	Moves the cursor forward one character.
Ctrl+K	Deletes from the cursor to the end of the command line.
Ctrl+L or Ctrl+R	Repeats the current command line on a new line.
Ctrl+N or Down Arrow key	Enters the next command line in the history buffer.
Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.

Downloaded from www.Manualslib.com manuals search engine

Table 4 Keyboard Shortcuts (continued)

Keyboard Shortcut(s)	Function
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs

The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to show the command(s) that begin with those characters. For example:

```
WX1200# display i <Tab>
ifm         display interfaces maintained by the interface
manager
igmp        display igmp information
interface   display interfaces
ip          display ip information
```

Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*****) wildcard character in globbing. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 26.)

Double-Asterisk (**) Wildcard Characters

The double-asterisk (******) wildcard character matches all usernames. For details, see "User Globs" on page 26.

Downloaded from www.Manualslib.com manuals search engine

Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the **help** command. For example:

```
WX1200# help
Commands:
--------------------------------------------------------------------------
clear                 Clear, use 'clear help' for more information
commit                Commit the content of the ACL table
copy                  Copy from filename (or url) to filename (or url)
crypto                Crypto, use 'crypto help' for more information
delete                Delete url
dir                   Show list of files on flash device
disable               Disable privileged mode
display               Display, use 'display help' for more information
exit                  Exit from the Admin session
help                  Show this help screen
history               Show contents of history substitution buffer
load                  Load, use 'load help' for more information
logout                Exit from the Admin session
monitor               Monitor, use 'monitor help' for more information
ping                  Send echo packets to hosts
quit                  Exit from the Admin session
reset                 Reset, use 'reset help' for more information
rollback              Remove changes to the edited ACL table
save                  Save the running configuration to persistent storage
set                   Set, use 'set help' for more information
telnet                telnet IP address [server port]
traceroute            Print the route packets take to network host
```

For more information on help, see “help” on page 46.

To see a subset of the online help, type the command for which you want more information. For example, to show all the commands that begin with the letter *i*, type the following command:

```
WX1200# display i?
ifm                   Show interfaces maintained by the interface manager
igmp                  Show igmp information
interface             Show interfaces
ip                    Show ip information
```

Downloaded from www.Manualslib.com manuals search engine

To see all the variations, type one of the commands followed by a question mark (?). For example:

```
WX1200# display ip ?
alias                 display ip aliases
dns                   display DNS status
https                 display ip https
route                 display ip route table
telnet                display ip telnet
```

To determine the port on which Telnet is running, type the following command:

```
WX1200# display ip telnet
Server Status                  Port
---------------------------------
Enabled                         23
```

Understanding Command Descriptions

Each command description in the *3Com Mobility System Software Command Reference* contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:

  set {**ap** | **dap**} *name*

  The **set** {**ap** | **dap**} *name* command has the following complete syntax:

  set {**ap** *port-list* | **dap** *dap-num*} **name** *name*

- A brief description of the command's functions.
- The full command syntax.
- Any command defaults.
- The command access, which is either *enabled* or *all*. *All* indicates that anyone can access this command. *Enabled* indicates that you must enter the enable password before entering the command.
- The command history, which identifies the MSS version in which the command was introduced and the version numbers of any subsequent updates.
- Special tips for command usage. These are omitted if the command requires no special usage.
- One or more examples of the command in context, with the appropriate system prompt and response.
- One or more related commands.

Downloaded from www.Manualslib.com manuals search engine

2 ACCESS COMMANDS

This chapter describes access commands used to control access to the Mobility Software System (MSS) command-line interface (CLI).

Commands by Usage

This chapter presents access services commands alphabetically. Use Table 5 to located commands in this chapter based on their use.

Table 5 Access Commands by Usage

Type	Command
Access Privileges	**enable** on page 34
	set enablepass on page 35
	disable on page 33
	quit on page 34

disable

Changes the CLI session from enabled mode to restricted access.

Syntax — **`disable`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command restricts access to the CLI for the current session:

```
WX1200# disable
WX1200>
```

See Also

- **enable** on page 34

Downloaded from www.Manualslib.com manuals search engine

enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

Syntax — **`enable`**

Access — All.

History — Introduced in MSS Version 3.0.

Usage — MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this WX switch with the **set enablepass** command.

Examples — The following command plus the enable password provides enabled access to the CLI for the current sessions:

```
WX1200> enable
Enter password: password
WX1200#
```

See Also

- **set enablepass** on page 35
- **set confirm** on page 52

quit

Exit from the CLI session.

Syntax — **`quit`**

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To end the administrator's session, type the following command:

```
WX1200> quit
```

Downloaded from www.Manualslib.com manuals search engine

set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the WX switch.

Syntax — **`set enablepass`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — After typing the **set enablepass** command, press Enter. If you are entering the first enable password on this WX switch, press Enter at the **Enter old password** prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the **Retype new password** prompt.

CAUTION: *Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.*

Examples — The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

```
WX1200# set enablepass
Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
Password changed
```

See Also

- **disable** on page 33
- **enable** on page 34

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

3 System Service Commands

Use system services commands to configure and monitor system information for a WX switch.

Commands by Usage

This chapter presents system service commands alphabetically. Use Table 6 to locate commands in this chapter based on their use.

Table 6 System Services Commands by Usage

Type	Command
Configuration	**quickstart** on page 48
Auto-Config	**set auto-config** on page 48
Display	**clear banner motd** on page 38
	quickstart on page 48
	display banner motd on page 41
	set confirm on page 52
	set length on page 53
System Identification	**set prompt** on page 54
	set system name on page 60
	set system location on page 59
	set system contact on page 55
	set system countrycode on page 56
	set system idle-timeout on page 58
	set system idle-timeout on page 58
	display load on page 43
	display system on page 43
	clear system on page 40

Downloaded from www.Manualslib.com manuals search engine

Table 6 System Services Commands by Usage (continued)

Type	Command
	clear prompt on page 39
Help	**help** on page 46
History	**history** on page 47
	clear history on page 39
License	**display license** on page 42
	set license on page 53
Technical Support	**display base-information** on page 41

clear banner motd

Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the wireless LAN switch.

Syntax — **`clear banner motd`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear a banner, type the following command:

```
WX4400# clear banner motd
success: change accepted
```

As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command: ***set banner motd ^^***

See Also

- **display banner motd** on page 41
- **quickstart** on page 48

Downloaded from www.Manualslib.com manuals search engine

clear history

Deletes the command history buffer for the current CLI session.

Syntax — **`clear history`**

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To clear the history buffer, type the following command:

```
WX4400# clear history
success: command buffer was flushed.
```

See Also

- **history** on page 47

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to its default.

Syntax — **`clear prompt`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
WX4400#
```

See Also

- **set prompt** on page 54. (For information about default prompts, see "Command Prompts" on page 24.)

Downloaded from www.Manualslib.com manuals search engine

clear system

Clears the system configuration of the specified information.

CAUTION: *If you change the IP address, any currently configured Mobility Domain operations cease. You must reset the Mobility Domain.*

Syntax — **`clear system`** [**`contact`** | **`countrycode`** | **`idle-timeout`** | **`ip-address`** | **`location`** | **`name`**]

- **`contact`** — Resets the name of contact person for the WX switch to null.
- **`countrycode`** — Resets the country code for the WX switch to null.
- **`idle-timeout`** — Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds).
- **`ip-address`** — Resets the IP address of the WX switch to null.
- **`location`** — Resets the location of the WX switch to null.
- **`name`** — Resets the name of the WX switch to the default system name, which is the model number.

Defaults — None.

Access — Enabled.

History — —Introduced in MSS Version 3.0. Option idle-timeout added in MSS Version 4.1.

Examples — To clear the location of the WX switch, type the following command:

```
WX4400# clear system location
success: change accepted.
```

See Also

- **display config** on page 574
- **display system** on page 43
- **set system contact** on page 55
- **set system countrycode** on page 56
- **set system idle-timeout** on page 58
- **set system idle-timeout** on page 58
- **set system location** on page 59

Downloaded from www.Manualslib.com manuals search engine

display banner motd

Shows the banner that was configured with the **set banner motd** command.

Syntax — **`display banner motd`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To show the banner with the message of the day, type the following command:

```
WX4400# display banner motd
hello world
```

See Also

- **clear banner motd** on page 38
- **quickstart** on page 48

display base-information

Provides an in-depth snapshot of the status of the wireless LAN switch, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

Syntax — **`display base-information`**
`[`**`file`** `[`*`subdirname/`*`]`*`filename`*`]`

- `[`*`subdirname/`*`]`*`filename`* — Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Enter this command before calling for Technical Support. See "Obtaining Support for your Product" on page 637 for more information.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display boot** on page 573
- **display config** on page 574
- **display license** on page 42
- **display system** on page 43
- **display version** on page 576

display license

Displays information about the license currently installed on the WX switch.

Syntax — **`display license`**

Defaults — None.

Access — All.

Examples — To view the WX switch license, type the following command:

```
WX4400# display license
Serial Number    : M8XE4IBB8DB10

License Number   : 245
License Key      : WXL-076E-93E9-62DA-54D8
Activation key   : WXA-3E04-4CC2-430D-B508
Feature          : 24 additional ports
Expires          : Never
```

The additional ports refers to the number of additional MAPs the switch can boot and actively manage.

See Also

- **set license** on page 53

Downloaded from www.Manualslib.com manuals search engine

display load

Displays CPU usage on a WX switch.

Syntax — **`display load`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — To display the CPU load recorded from the time the WX switch was booted, as well as from the previous time the **display load** command was run, type the following command:

```
WX4400# display load
System Load: overall: 2% delta: 5%
```

The overall field shows the CPU load as a percentage from the time the WX switch was booted. The delta field shows CPU load as a percentage from the last time the **display load** command was entered.

See Also

- **display system** on page 43

display system

Shows system information.

Syntax — **`display system`**

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

Examples — To show system information, type the following command:

```
WX4400# display system
================================================================================
 Product Name:       WX4400
 System Name:        WX-bldg3
 System Countrycode: US
 System Location:    first-floor-bldg3
 System Contact:     tamara@example.com
 System IP:          192.168.12.7
 System idle timeout: 3600
 System MAC:         00:0B:0E:00:04:30
================================================================================
 Boot Time:          2003-11-07 15:45:49
 Uptime:                 13 days 04:29:10
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      97.04/744.03 (13%)
 Total Power Over Ethernet : 29.000
================================================================================
```

Table 7 describes the fields of **display system output**.

Table 7 display system output

Field	Description
Product Name	Switch model number.
System Name	System name (factory default, or optionally configured with **set system name**).
System Countrycode	Country-specific 802.11 code required for MAP operation (configured with **set system countrycode**).
System Location	Record of the WX switch's physical location (optionally configured with **set system location**).
System Contact	Contact information about the system administrator or another person to contact about the system (optionally configured with **set system contact**).
System IP	Common interface, source, and default IP address for the device, in dotted decimal notation (configured with **set system ip-address**).

Downloaded from www.Manualslib.com manuals search engine

Table 7 display system output (continued)

Field	Description
System idle timeout	Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the **set system idle-timeout** command.)
System MAC	WX switch's media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.
License	License level installed on the WX switch (if applicable).
Boot Time	Date and time of the last system reboot.
Uptime	Number of days, hours, minutes, and seconds that the WX has been operating since its last restart.
Fan status	Operating status of the WX switch's three cooling fans: ▪ **OK** — Fan is operating. ▪ **Failed** — Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected. Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back.
Temperature	Status of temperature sensors at three locations in the WX switch: ▪ **ok** — Temperature is within the acceptable range of 0° C to 50° C (32° F to 122° F). ▪ **Alarm** — Temperature is above or below the acceptable range. MSS sends an alert to the system log every 5 minutes until this condition is corrected.
PSU Status	Status of the lower and upper power supply units: ▪ **missing** — Power supply is not installed or is inoperable. ▪ **DC ok** — Power supply is producing DC power. ▪ **DC output failure** — Power supply is not producing DC power. MSS sends an alert to the system log every 5 minutes until this condition is corrected. ▪ **AC ok** — Power supply is receiving AC power. ▪ **AC not present** — Power supply is not receiving AC power.

Downloaded from www.Manualslib.com manuals search engine

Table 7 display system output (continued)

Field	Description
Memory	Current size (in megabytes) of nonvolatile memory (NVRAM) and synchronous dynamic RAM (SDRAM), plus the percentage of total memory space in use, in the following format: *NVRAM size*/*SDRAM size (percent of total)*
Total Power Over Ethernet	Total power that the device is currently supplying to its directly connected MAP access points, in watts.

See Also

- **clear system** on page 40
- **set system contact** on page 55
- **set system countrycode** on page 56
- **set system idle-timeout** on page 58
- **set system location** on page 59
- **set system name** on page 60

help

Displays a list of commands that can be used to configure and monitor the WX switch.

Syntax — **`help`**

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To show a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

```
WX4400# help
Commands:
--------------------------------------------------------------------------
clear                  Clear,  use 'clear help' for more information
commit                 Commit the content of the ACL table
copy                   Copy from filename (or url) to filename (or url)
```

Downloaded from www.Manualslib.com manuals search engine

```
crypto                  Crypto, use 'crypto help' for more information
delete                  Delete url
dir                     Show list of files on flash device
disable                 Disable privileged mode
display                 Display, use 'display help' for more information
exit                    Exit from the Admin session
help                    Show this help screen
history                 Show contents of history substitution buffer
hit-sample-rate         Set NP hit-counter sample rate
load                    Load, use 'load help' for more information
logout                  Exit from the Admin session
monitor                 Monitor, use 'monitor help' for more information
ping                    Send echo packets to hosts
quit                    Exit from the Admin session
reset                   Reset, use 'reset help' for more information
rollback                Remove changes to the edited ACL table
save                    Save the running configuration to persistent storage
set                     Set, use 'set help' for more information
telnet                  telnet IP address [server port]
traceroute              Print the route packets take to network host
```

See Also

- **Using CLI Help** on page 31

history

Displays the command history buffer for the current CLI session.

Syntax — **`history`**

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To show the history of your session, type the following command:

```
WX4400> history
Show History (most recent first)
--------------------------------
[00] display config
[01] display version
[02] enable
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear history** on page 39

---

quickstart

Runs a script that interactively helps you configure a new switch.

(For more information, see the "CLI quickstart Command" section of the "WX Setup Methods" chapter in the *Wireless LAN Switch and Controller Configuration Guide*.)

CAUTION: *The quickstart command is for configuration of a new switch only. After prompting you for verification, the command erases the switch's configuration before continuing. If you run this command on a switch that already has a configuration, the configuration will be erased. In addition, error messages such as "Critical AP Notice" for directly connected MAPs can appear.*

---

set auto-config

Enables a WX switch to contact a 3WXM server for its configuration.

Syntax — **`set auto-config {enable | disable}`**

- **`enable`** — Enables the switch to contact a 3WXM server to request a configuration.
- **`disable`**— Disables the auto-config option.

Defaults — The auto-config option is automatically enabled on an unconfigured WXR100 when the factory reset switch is pressed during power on. However, auto-config is disabled by default on other models.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — A network administrator at the corporate office can preconfigure the switch in a 3WXM network plan. The switch configuration must have a name for the switch, the model must be WXR100, and the serial number must match the switch's serial number. The configuration should also include all other settings required for the deployment, including MAP configuration, SSIDs, AAA settings, and so on.

Downloaded from www.Manualslib.com manuals search engine

When the 3WXM server in the corporate network receives the configuration request, the server looks in the currently open network plan for a switch configuration with the same model and serial number as the one in the configuration request.

- If the network plan contains a configuration with a matching model and serial number, 3WXM sends the configuration to the switch and restarts the switch. The switch boots using the configuration it received from 3WXM.
- If the network plan does not have a configuration with a matching model and serial number, a verification warning appears in 3WXM. The warning lists the switch's serial number and IP address. The network administrator can upload the switch into the network plan, configure switch parameters, and deploy the configuration to the switch.

To use the auto-config option with a new (unconfigured) WXR100, insert a paperclip or similar object into the WXR100's factory reset hole to press the switch. The factory reset switch must be held for about 3 seconds while the factory reset LED (the right LED above port 1) is lit. Normally, this LED remains solidly lit for 3 seconds after power on. However, when the factory reset switch is pressed, the LED flashes for 3 seconds instead.

If you want another WX switch model to be able to access a 3WXM server for a configuration, you also must preconfigure the WX with the following information:

- IP address
- Gateway address
- Domain name and DNS server address

You can enable the switch to use the MSS DHCP client to obtain this information from a DHCP server in the local network where the switch will be deployed. Alternatively, you can statically configure the information.

The IP address and DNS information are configured independently. You can configure the combination of settings that work with the network resources available at the deployment site. The following examples show some of the combinations you can configure.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands stage a WX switch to use the auto-config option. The network where the switch is installed has a DHCP server, so the switch is configured to use the MSS DHCP client to obtain an IP address, default gateway address, DNS domain name, and DNS server IP addresses:

1 Configure a VLAN:

```
WX-1200# set vlan 1 port 7
success: change accepted.
```

2 Enable the DHCP client on VLAN 1:

```
WX-1200# set interface 1 ip dhcp-client enable
success: change accepted.
```

3 Enable the auto-config option:

```
WX-1200# set auto-config enable
success: change accepted.
```

4 Create a self-signed administrative certificate, to enable the WX to communicate with the 3WXM server.

```
WX-1200# crypto generate key admin 1024
key pair generated
WX-1200# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name: remoteswitch1@example.com
Email Address:
Unstructured Name:
Self-signed cert for admin is
-----BEGIN CERTIFICATE-----
MIICUzCCAbygAwIBAgICA+cwDQYJKoZIhvcNAQEEBQAwNjELMAkGA1UEBhMC
VVMx
CzAJBgNVBAgTAkNBMRowGAYDVQQDFBF0ZWNocHVic0B0cnB6LmNvbTAeFw0w
MzA0
...
Lm8wmVYLxP56MpCUAm9O8C2foYgOY40=
-----END CERTIFICATE-----
```

5 Save the configuration changes:

```
WX-1200# save config
success: configuration saved.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **crypto generate key** on page 473
- **crypto generate self-signed** on page 476
- **save config** on page 584
- **set interface dhcp-client** on page 161
- **set vlan port** on page 117

set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the WX switch.

Syntax — **`set banner motd ^`***`text`***`^`**

- **^** — Delimiting character that begins and ends the message.
- *`text`* — Up to 2000 alphanumeric characters, including tabs and carriage returns, but *not* the delimiting character (**^**). The maximum number of characters is approximately 24 lines by 80 characters.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Type a caret (**^**), then the message, then another caret.

Do not use the following characters with commands in which you set text to be displayed on the WX switch, such as message-of-the-day (MOTD) banners:

- Ampersand (&)
- Angle brackets (< >)
- Double quotation marks (" ")
- Number sign (#)
- Question mark (?)
- Single quotation mark (')

Downloaded from www.Manualslib.com manuals search engine

Examples — To create a banner that says *Update meeting at 3 p.m.,* type the following command:

```
WX4400# set banner motd ^Update meeting at 3 p.m.^
success: change accepted.
```

See Also

- **clear banner motd** on page 38
- **display banner motd** on page 41

set confirm

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

Syntax — **set confirm** {**on** | **off**}

- **on** — Enables confirmation messages.
- **off** — Disables confirmation messages.

Defaults — Configuration messages are enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command remains in effect for the duration of the session, until you enter a **quit** command, or until you enter another **set confirm** command.

MSS displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
WX4400# clear vlan red
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]
```

Examples — To turn off these confirmation messages, type the following command:

```
WX4400# set confirm off
success: Confirm state is off
```

Downloaded from www.Manualslib.com manuals search engine

set length

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

Syntax — **`set length`** *`number-of-lines`*

- *`number-of-lines`* — Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

Defaults — MSS displays 24 lines by default.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

Examples — To set the number of lines displayed to 100, type the following command:

```
WX4400# set length 100
success: screen length for this session set to 100
```

set license

Installs an upgrade license, for managing more MAPs.

Syntax — **`set license`** *`license-key activation-key`*

- *`license-key`* — License key, starting with WXL. You can enter the key with or without the hyphens.
- *`activation-key`* — Activation key, starting with WXA. You can enter the key with or without the hyphens.

Defaults — The WX4400 can boot and manage 24 MAPs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — The license key is shipped with the switch. To obtain the activation key, access the 3Com web site. Each license and activation key pair allows the switch to actively manage an additional 24 MAPs. You can install up to three upgrade license and activation key pairs, to actively manage up to 96 MAPs.

Examples — To install an upgrade license and activation key, type the following command:

```
WX4400# set license WXL-076E-93E9-62DA-54D8
WXA-3E04-4CC2-430D-B508
Serial Number    : M8XE4IBB8DB10

License Number   : 245
License Key      : WXL-076E-93E9-62DA-54D8
Activation key   : WXA-3E04-4CC2-430D-B508
Feature          : 24 additional ports
Expires          : Never

48 ports are enabled
success: license was installed
```

The additional ports refers to the number of additional MAPs the switch can boot and actively manage.

See Also

- **display license** on page 42

set prompt

Changes the CLI prompt for the WX switch to a string you specify.

Syntax — **`set prompt`** *`string`*

- *`string`* — Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks (**“”**).

Defaults — The factory default for the WX switch name is the model number (*WX1200* for the 3Com Wireless LAN Switch WX1200, *WX4400* for the 3Com Wireless LAN Controller WX4400).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — When you first log in for the initial configuration of the WX switch, the CLI provides a *WX1200*> or *WX4400*> prompt, depending on your model. After you become enabled by typing **enable** and giving a suitable password, the *WX1200*# or *WX4400*# prompt is displayed.

If you use the **set system name** command to change the default system name, MSS uses that name in the prompt, unless you also change the prompt with **set prompt**.

Examples — The following example sets the prompt from *WX4400* to *happy_days*:

```
WX4400# set prompt happy_days
success: change accepted.
happy_days#
```

See Also

- **clear prompt** on page 39
- **display config** on page 574
- **set system name** on page 60

set system contact

Stores a contact name for the WX switch.

Syntax — **set system contact** *string*

- *string* — Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

To view the system contact string, type the **display system** command.

Examples — The following command sets the system contact information to *tamara@example.com*:

```
WX1200# set system contact tamara@example.com
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear system** on page 40
- **display system** on page 43
- **set system location** on page 59
- **set system name** on page 60

set system countrycode

Defines the country-specific IEEE 802.11 regulations to enforce on the WX switch.

Syntax — **`set system countrycode`** *`code`*

- *`code`* — Two-letter code for the country of operation for the WX switch. You can specify one of the codes listed in Table 8.

Table 8 Country Codes

Country	Code
Australia	AU
Austria	AT
Belgium	BE
Brazil	BR
Canada	CA
China	CN
Czech Republic	CZ
Denmark	DK
Finland	FI
France	FR
Germany	DE
Greece	GR
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Ireland	IE
Israel	IL
Italy	IT

Downloaded from www.Manualslib.com manuals search engine

Table 8 Country Codes (continued)

Country	Code
Japan	JP
Liechtenstein	LI
Luxembourg	LU
Malaysia	MY
Mexico	MX
Netherlands	NL
New Zealand	NZ
Norway	NO
Poland	PL
Portugal	PT
Saudi Arabia	SA
Singapore	SG
Slovakia	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH
United Arab Emirates	AE
United Kingdom	GB
United States	US

Defaults — The factory default country code is None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must set the system county code to a valid value before using any **set ap** commands to configure a MAP.

Downloaded from www.Manualslib.com manuals search engine

Examples — To set the country code to Canada, type the following command:

```
WX1200# set system country code CA
success: change accepted.
```

See Also

- **display config** on page 574

---

set system idle-timeout

Specifies the maximum number of seconds a CLI management session with the switch can remain idle before MSS terminates the session.

Syntax — **set system idle-timeout** *seconds*

- *seconds* — Number of seconds a CLI management session can remain idle before MSS terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled.

Defaults — 3600 seconds (one hour).

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions and new sessions.

Examples — The following command sets the idle timeout to 1800 seconds (one half hour):

```
WX1200# set system idle-timeout 1800
success: change accepted.
```

See Also

- **clear system** on page 40
- **display system** on page 43

Downloaded from www.Manualslib.com manuals search engine

set system ip-address

Sets the system IP address so that it can be used by various services in the WX switch.

CAUTION: *Any currently configured Mobility Domain operations cease if you change the IP address. If you change the address, you must reset the Mobility Domain.*

Syntax — **`set system ip-address`** *`ip-addr`*

- *`ip-addr`* — IP address, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the IP address of the WX switch to 192.168.253.1:

```
WX4400# set system ip-address 192.168.253.1
success: change accepted.
```

See Also

- **clear system** on page 40
- **set interface** on page 160
- **display system** on page 43

set system location

Stores location information for the WX switch.

Syntax — **`set system location`** *`string`*

- *`string`* — Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot include spaces in the system location string.

Downloaded from www.Manualslib.com manuals search engine

To view the system location string, type the **display system** command.

Examples — To store the location of the WX switch in the WX's configuration, type the following command:

```
WX4400# set system location first-floor-bldg3
success: change accepted.
```

See Also

- **clear system** on page 40
- **display system** on page 43
- **set system contact** on page 55
- **set system name** on page 60

set system name

Changes the name of the WX switch from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

Syntax — **set system name** *string*

- *string* — Alphanumeric string up to 256 characters long, with no blank spaces. Use a unique name for each WX switch.

Defaults — By default, the system name and command prompt have the same value. The factory default for both is the model number (*WX1200* for the 3Com Wireless LAN Switch WX1200, *WX4400* for the 3Com Wireless LAN Controller WX4400).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Entering **set system name** with no string resets the system name to the factory default.

To view the system name string, type the **display system** command.

Examples — The following example sets the system name to a name that identifies the WX switch:

```
WX4400# set system name WX-bldg3
success: change accepted.
WX-bldg3#
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear system** on page 40
- **display system** on page 43
- **set prompt** on page 54
- **set system contact** on page 55
- **set system location** on page 59

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

4 PORT COMMANDS

Use port commands to configure and manage individual ports and load-sharing port groups.

Commands by Usage

This chapter presents port commands alphabetically. Use Table 9 to locate commands in this chapter based on their use.

Table 9 Port Commands by Usage

Type	Command
Port Type	**set port type ap** on page 91
	set dap on page 81
	set port type wired-auth on page 94
	clear port type on page 68
	clear dap on page 64
Name	**set port name** on page 86
	clear port name on page 66
State	**set port** on page 83
	reset port on page 81
	display port status on page 73
Gigabit Interface Type	**display port media-type** on page 75
	set port media-type on page 85
	clear port media-type on page 66
Speed	**set port speed** on page 89
Autonegotiation	**set port negotiation** on page 86
PoE	**set port poe** on page 87
	display port poe on page 71
SNMP	**set port trap** on page 90

Downloaded from www.Manualslib.com manuals search engine

Table 9 Port Commands by Usage (continued)

Type	Command
Port Groups	**set port-group** on page 84
	display port-group on page 70
	clear port-group on page 65
Statistics	**display port counters** on page 69
	monitor port counters on page 76
	clear port counters on page 65

clear dap

Removes a Distributed MAP.

CAUTION: *When you clear a Distributed MAP, MSS ends user sessions that are using the MAP.*

Syntax — **`clear dap`** *`dap-num`*

- *`dap-num`* — Number of the Distributed MAP(s) you want to remove.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears Distributed MAP 1:

```
WX4400# clear dap 1
This will clear specified DAP devices.
Would you like to continue? (y/n) [n]y
```

See Also

- **set dap** on page 81
- **set port type ap** on page 91

Downloaded from www.Manualslib.com manuals search engine

clear port counters

Clears port statistics counters and resets them to 0.

Syntax — **`clear port counters`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears all port statistics counters and resets them to 0:

```
WX4400# clear port counters
success: cleared port counters
```

See Also

- **display port counters** on page 69
- **monitor port counters** on page 76

clear port-group

Removes a port group.

Syntax — **`clear port-group name`** *`name`*

- **`name`** *`name`* — Name of the port group.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears port group server1:

```
WX4400# clear port-group name server1
success: change accepted.
```

See Also

- **set port-group** on page 84
- **display port-group** on page 70

Downloaded from www.Manualslib.com manuals search engine

clear port media-type

Disables the copper interface and reenables the fiber interface on an WX4400 gigabit Ethernet port.

Syntax — **`clear port media-type`** *`port-list`*

- *`port-list`*—List of physical ports. MSS disables the copper interface and reenables the fiber interface on all the specified ports.

Defaults — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

Examples — The following command disables the copper interface and reenables the fiber interface on port 2:

```
WX4400# clear port media-type 2
```

See Also

- **set port media-type** on page 85
- **display port media-type** on page 75

clear port name

Removes the name assigned to a port.

Syntax — **`clear port`** *`port-list`* **`name`**

- *`port-list`* — List of physical ports. MSS removes the names from all the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command clears the names of ports 1 through 3:

```
WX4400# clear port 1-3 name
```

See Also

- **display port status** on page 73
- **set port name** on page 86

clear port preference

Resets a gigabit Ethernet port on a WX4400 to use the GBIC (fiber) interface for the active link.

Syntax — **clear port preference** *port-list*

- *port-list* — List of physical ports. MSS clears the preference on all the specified ports.

Defaults — When both the copper and fiber interfaces of a gigabit Ethernet port are connected, the GBIC (fiber) interface is the active link. The RJ-45 (copper) link is unused.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

Examples — The following command clears the preference set on port 2 on a WX4400 switch:

```
WX4400# clear port preference 2
```

See Also

- **display port preference** on page 72
- **set port preference** on page 88

Downloaded from www.Manualslib.com manuals search engine

clear port type

Removes all configuration settings from a port and resets the port as a network port.

CAUTION: *When you clear a port, MSS ends user sessions that are using the port.*

Syntax — **`clear port type`** *`port-list`*

- *`port-list`* — List of physical ports. MSS resets and removes the configuration from all the specified ports.

Defaults — The cleared port becomes a network port but is not placed in any VLANs.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear a MAP access point port, all MAP-specific settings are removed. Table 10 lists the default network port settings that MSS applies when you clear a port's type.

Table 10 Network port defaults

Port Parameter	Setting
VLAN membership	None. **Note:** Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN.
Spanning Tree Protocol (STP)	Based on the VLAN(s) you add the port to.
802.1X	No authorization.
Port groups	None.
Internet Group Management Protocol (IGMP) snooping	Enabled as port is added to VLANs.
Access point and radio parameters	Not applicable
Maximum user sessions	Not applicable

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command clears port 5:

```
WX1200# clear port type 5
This may disrupt currently authenticated users.
Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- **set port type ap** on page 91
- **set port type wired-auth** on page 94

display port counters

Displays port statistics.

Syntax — **display port counters** [**octets** | **packets** | **receive-errors** | **transmit-errors** | **collisions** | **receive-etherstats** | **transmit-etherstats**] [**port** *port-list*]

- **octets** — Shows octet statistics.
- **packets** — Shows packet statistics.
- **receive-errors**— Shows errors in received packets.
- **transmit-errors** — Shows errors in transmitted packets.
- **collisions** — Shows collision statistics.
- **receive-etherstats** — Shows Ethernet statistics for received packets.
- **transmit-etherstats** — Shows Ethernet statistics for transmitted packets.
- **port** *port-list* — List of physical ports. If you do not specify a port list, MSS shows statistics for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — You can specify one statistic type with the command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows octet statistics for port 3:

```
WX1200> display port counters octets port 3
Port   Status                    Rx Octets                      Tx Octets
================================================================================
    3    Up                        27965420                       34886544
```

This command's output has the same fields as the **monitor port counters** command. For descriptions of the fields, see Table 17 on page 78.

See Also

- **clear port counters** on page 65
- **monitor port counters** on page 76

display port-group

Shows port group information.

Syntax — **display port-group** [**all** | **name group-name**]

- **all** — Shows information for all port groups.
- **name** *group-name* — Shows information for the specified port group.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the configuration of port group server2:

```
WX1200# display port-group name server2
Port group: server2 is up
        Ports: 5, 7
```

Table 11 describes the fields in the display port-group output.

Table 11 Output for display port-group

Field	Description
Port group	Name and state (enabled or disabled) of the port group.
Ports	Ports contained in the port group.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear port-group** on page 65
- **set port-group** on page 84

display port poe

Displays status information for ports on which Power over Ethernet (PoE) is enabled.

Syntax — **display port poe** [*port-list*]

- *port-list* — List of physical ports. If you do not specify a port list, PoE information is displayed for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays PoE information for all ports on a WX1200 switch:

```
WX1200# display port poe
              Link     Port    PoE        PoE
Port  Name            Status   Type    config    Draw
=============================================================
   1  1                up       -     disabled  off
   2  2                down     -     disabled  off
   3  3                down     -     disabled  off
   4  4                down     MAP   enabled  1.44
   5  5                down     -     disabled  off
   6  6                down     -     disabled  off
```

Table 12 describes the fields in this display.

Table 12 Output for display port poe

Field	Description
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.

Downloaded from www.Manualslib.com manuals search engine

Table 12 Output for display port poe (continued)

Field	Description
Link status	Link status of the port: ▪ **up**—The port is connected. ▪ **down**—The port is not connected.
Port type	Port type: ▪ **MAP** —The port is a MAP access port. ▪ **-** (The port is not a MAP access port.)
PoE config	PoE state: ▪ enabled ▪ disabled
PoE Draw	Power draw on the port, in watts. For 10/100 Ethernet ports on which PoE is disabled, this field displays *off*. For gigabit Ethernet ports, this field displays *invalid*, because PoE is not supported on gigabit Ethernet ports. The value *overcurrent* indicates a PoE problem such as a short in the cable.

See Also

- **set port poe** on page 87

display port preference

Displays the interface preferences set on WX4400 gigabit Ethernet ports.

Syntax — **`display port preference`** [*`port-list`*]

- *`port-list`* — List of physical ports. MSS displays the preference for all the specified ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the WX4400.

Examples — The following command displays the preference settings on all four ports of a WX4400 switch:

```
WX4400# display port preference
```

Downloaded from www.Manualslib.com manuals search engine

```
Port  Preference
============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

Table 13 describes the fields in this display.

Table 13 Output for display port preference

Field	Description
Port	Port number.
Preference	Preference setting: ▪ **GBIC** — The GBIC (fiber) interface is selected as the active interface. ▪ **RJ45** — The RJ-45 (copper) interface is selected as the active interface.

See Also

- **clear port preference** on page 67
- **set port preference** on page 88

display port status

Displays configuration and status information for ports.

Syntax — **`display port status`** [*`port-list`*]

- *`port-list`* — List of physical ports. If you do not specify a port list, information is displayed for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays information for all ports on a WX1200 switch:

```
WX1200# display port status
Port  Name             Admin  Oper   Config     Actual    Type        Media
================================================================================
   1  1                up     up      auto      100/full  network    10/100BaseTx
   2  2           up     up      auto      100/full  ap         10/100BaseTx
   3  3           up     up      auto      100/full  network    10/100BaseTx
   4  4                up     down    auto                network    10/100BaseTx
   5  5                up     down    auto                network    10/100BaseTx
   6  6                up     down    auto                network    10/100BaseTx
   7  7                up     down    auto                network    10/100BaseTx
   8  8                up     down    auto                network    10/100BaseTx
```

Table 14 describes the fields in this display.

Table 14 Output for display port status

Field	Description
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.
Admin	Administrative status of the port: ▪ **up** — The port is enabled. ▪ **down** — The port is disabled.
Oper	Operational status of the port: ▪ **up** — The port is operational. ▪ **down** — The port is not operational.
Config	Port speed configured on the port: ▪ **10** — 10 Mbps. ▪ **100** — 100 Mbps. ▪ **1000** — 1000 Mbps. ▪ **auto** — The port sets its own speed.
Actual	Speed and operating mode in effect on the port.
Type	Port type: ▪ **ap** — MAP access point port ▪ **network** — Network port ▪ **wa** — Wired authentication port

Downloaded from www.Manualslib.com manuals search engine

Table 14 Output for display port status (continued)

Field	Description
Media	Link type: **10/100BaseTX** — 10/100BASE-T. **GBIC** — 1000BASE-SX or 1000BASE-LX GBIC. **1000BaseT** — 1000BASE-T. **No connector** — GBIC slot is empty.

See Also

- **clear port type** on page 68
- **set port** on page 83
- **set port name** on page 86
- **set port negotiation** on page 86
- **set port speed** on page 89
- **set port type ap** on page 91
- **set port type wired-auth** on page 94

display port media-type

Displays the enabled interface types on a WX4400 switch's gigabit Ethernet ports.

See Also — **`display port media-type [`***`port-list`***`]`**

- *`port-list`* — List of physical ports. MSS displays the enabled interface types for all the specified ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400.

Examples — The following command displays the enabled interface types on all four ports of a WX4400 switch:

```
WX4400# display port media-type
Port  Media Type
```

Downloaded from www.Manualslib.com manuals search engine

```
=============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

Table describes the fields in this display.

Table 15 Output for display port media-type

Field	Description
Port	Port number.
Preference	Preference setting: GBIC—The GBIC (fiber) interface is enabled. RJ45—The RJ-45 (copper) interface is enabled.

See Also

- **clear port media-type** on page 66
- **set port media-type** on page 85

monitor port counters

Displays and continually updates port statistics.

Syntax — **monitor port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats]**

- **octets** — Displays octet statistics first.
- **packets** — Displays packet statistics first.
- **receive-errors** — Displays errors in received packets first.
- **transmit-errors** — Displays errors in transmitted packets first.
- **collisions** — Displays collision statistics first.
- **receive-etherstats** — Displays Ethernet statistics for received packets first.
- **transmit-etherstats** — Displays Ethernet statistics for transmitted packets first.

Downloaded from www.Manualslib.com manuals search engine

Defaults — All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds. This interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

Access — All.

History—Introduced in MSS Version 3.0.

Usage — Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 16 to control the monitor display.

Table 16 Key Controls for Monitor Port Counters Display

Field	Description
Spacebar	Advances to the next statistic type.
Esc	Exits the monitor. MSS stops displaying the statistics and displays a new command prompt.
c	Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.

For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command starts the port statistics monitor beginning with octet statistics (the default):

```
WX4400# monitor port counters
```

As soon as you press Enter, MSS clears the window and displays statistics at the top of the window.

```
Port   Status                        Rx Octets                          Tx Octets
================================================================================
    1  Up                          27965420                         34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port   Status     Rx Unicast    Rx NonUnicast       Tx Unicast     Tx NonUnicast
================================================================================
    1  Up            54620           62144           68318            62556
...
```

Table 17 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

Table 17 Output for monitor port counters

Statistics Option	Field	Description
Displayed for All Options	Port	Port the statistics are displayed for.
	Status	Port status. The status can be Up or Down.
octets	Rx Octets	Total number of octets received by the port. This number includes octets received in frames that contained errors.
	Tx Octets	Total number of octets received. This number includes octets received in frames that contained errors.

Downloaded from www.Manualslib.com manuals search engine

Table 17 Output for monitor port counters (continued)

Statistics Option	Field	Description
packets	Rx Unicast	Number of unicast packets received. This number does not include packets that contain errors.
	Rx NonUnicast	Number of broadcast and multicast packets received. This number does not include packets that contain errors.
	Tx Unicast	Number of unicast packets transmitted. This number does not include packets that contain errors.
	Tx NonUnicast	Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.
receive-errors	Rx Crc	Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.
	Rx Error	Total number of frames received in which the Physical layer (PHY) detected an error.
	Rx Short	Number of frames received by the port that were fewer than 64 bytes long.
	Rx Overrun	Number of frames received by the port that were valid but were longer than 1518 bytes. This statistic does not include jumbo packets with valid CRCs.
transmit-errors	Tx Crc	Number of frames transmitted by the port that had the correct length but contained an invalid FCS value.
	Tx Short	Number of frames transmitted by the port that were fewer than 64 bytes long.
	Tx Fragment	Total number of frames transmitted that were less than 64 octets long and had invalid CRCs.
	Tx Abort	Total number of frames that had a link pointer parity error.

Downloaded from www.Manualslib.com manuals search engine

Table 17 Output for monitor port counters (continued)

Statistics Option	Field	Description
collisions	Single Coll	Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network.
	Multiple Coll	Total number of frames transmitted that experienced more than one collision before 64 bytes of the frame were transmitted on the network.
	Excessive Coll	Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted.
	Total Coll	Best estimate of the total number of collisions on this Ethernet segment.
receive-etherstats	Rx 64	Number of packets received that were 64 bytes long.
	Rx 127	Number of packets received that were from 65 through 127 bytes long.
	Rx 255	Number of packets received that were from 128 through 255 bytes long.
	Rx 511	Number of packets received that were from 256 through 511 bytes long.
	Rx 1023	Number of packets received that were from 512 through 1023 bytes long.
	Rx 1518	Number of packets received that were from 1024 through 1518 bytes long.
transmit-etherstats	Tx 64	Number of packets transmitted that were 64 bytes long.
	Tx 127	Number of packets transmitted that were from 65 through 127 bytes long.
	Tx 255	Number of packets transmitted that were from 128 through 255 bytes long.
	Tx 511	Number of packets transmitted that were from 256 through 511 bytes long.
	Tx 1023	Number of packets transmitted that were from 512 through 1023 bytes long.
	Tx 1518	Number of packets transmitted that were from 1024 through 1518 bytes long.

See Also

- **display port counters** on page 69

Downloaded from www.Manualslib.com manuals search engine

reset port

Resets a port by toggling its link state and Power over Ethernet (PoE) state.

Syntax — **`reset port`** *`port-list`*

- *`port-list`* — List of physical ports. MSS resets all the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The reset command disables the port's link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing a MAP access point that is connected to two WX switches to reboot over the link to the other switch.

Examples — The following command resets port 5:

```
WX1200# reset port 5
```

See Also

- **set port** on page 83

set dap

Configures a Distributed MAP for a MAP access point that is indirectly connected to the WX switch through an intermediate Layer 2 or Layer 3 network.

*Before configuring a Distributed MAP, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the WX switch. See "set system countrycode" on page 56.*

*For a MAP that is directly connected to the WX switch, use the **set port type ap** command to configure a MAP access port.*

Syntax — **`set dap`** *`dap-num`* **`serial-id`** *`serial-ID`* **`model`** {**`ap2750`** | **`ap3750`**| **`ap7250`** | **`ap8250`** | **`ap8750`** | **`mp-52`** | **`mp-241`** | **`mp-252`** | **`mp-262`** | **`mp-341`** | **`mp-352`** | **`mp-372`** | **`mp-372-CN`** | **`mp-37-JP`** | **`mp-620`**} [**`radiotype`** {**`11a`** | **`11b`** | **`11g`**}]

Downloaded from www.Manualslib.com manuals search engine

- *dap-num* — Number for the Distributed MAP. The range of valid connection numbers depends on the WX switch model:
  - For a WX4400, you can specify a number from 1 to 256.
  - For a WX1200, you can specify a number from 1 to 30.
- **serial-id** *serial-ID* — MAP access point serial ID. The serial ID is listed on the MAP case. To show the serial ID using the CLI, use the **display version details** command.
- **radiotype 11a | 11b| 11g** — Radio type:
  - **11a** — 802.11a
  - **11b** — 802.11b
  - **11g** — 802.11g

  This option applies only to single-radio models.

Defaults — The default values are the same as the defaults for the **set port type ap** command.

Access — Enabled.

History — Introduced in MSS Version 3.0. New values for model option added in Version 4.1:

- AP3750
- AP2750
- mp-620

Examples — The following command configures Distributed MAP 1 for MAP model AP2750 with serial-ID M9DE48B012F00:

```
WX4400# set dap 1 serial-id M9DE48B012F00 model ap2750
success: change accepted.
```

The following command removes Distributed MAP 1:

```
WX4400# clear dap 1
This will clear specified DAP devices.
Would you like to continue? (y/n) [n]y
```

See Also

- **clear dap** on page 64

Downloaded from www.Manualslib.com manuals search engine

- **clear port type** on page 68
- **set port type ap** on page 91
- **set radio-profile 11g-only** on page 347
- **set system countrycode** on page 56

---

set port

Administratively disables or reenables a port.

Syntax — **`set port`** {**`enable`** | **`disable`**} *`port-list`*

- **`enable`** — Enables the specified ports.
- **`disable`** — Disables the specified ports.
- *`port-list`* — List of physical ports. MSS disables or reenables all the specified ports.

Defaults — All ports are enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Examples — The following command disables port 6:

```
WX1200# set port disable 6
success: set "disable" on port 6
```

The fol1owing command reenables the port:

```
WX1200# set port enable 6
success: set "enable" on port 6
```

See Also

- **reset port** on page 81

Downloaded from www.Manualslib.com manuals search engine

set port-group

Configures a load-sharing port group. All ports in the group function as a single logical link.

Syntax — **set port-group name** *group-name port-list* **mode** {**on** | **off**}

- **name** *group-name* — Alphanumeric string of up to 255 characters, with no spaces.
- *port-list* — List of physical ports. All the ports you specify are configured together as a single logical link.
- **mode** {**on** | **off**} — State of the group. Use **on** to enable the group or **off** to disable the group. The group is enabled by default.

Defaults — Once configured, a group is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure up to 8 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports and gigabit Ethernet ports in the same port group.

After you add a port to a port group, you cannot configure port parameters on the individual port. Instead, change port parameters on the entire group. Specify the group name instead of an individual port name or number in port configuration commands.

To add or remove ports in a group that is already configured, change the mode to off, add or remove the ports, then change the mode to on.

Examples — The following command configures a port group named server1 containing ports 1 through 5, and enables the link:

```
WX1200# set port-group name server1 1-5 mode on
success: change accepted.
```

The following commands disable the link for port group *server1,* change the list of ports in the group, and reenable the link:

```
WX1200# set port-group name server1 1-5 mode off
success: change accepted.
WX1200# set port-group name server1 1-4,7 mode on
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear port-group** on page 65
- **display port-group** on page 70

---

set port media-type

Disables the fiber interface and enables the copper interface on an WX4400 gigabit Ethernet port.

Syntax — `set port media-type` *`port-list`* `rj45`

- *`port-list`*—List of physical ports. MSS sets the preference on all the specified ports.
- **`rj45`**—Uses the copper interface.

Defaults — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400.

If you set the port interface to RJ-45 on a port that already has an active fiber link, MSS immediately changes the link to the copper interface.

Examples — The following command disables the fiber interface and enables the copper interface on port 2:

```
WX4400# set port media-type 2 rj45
```

See Also

- **clear port media-type** on page 66
- **display port media-type** on page 75

Downloaded from www.Manualslib.com manuals search engine

set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

Syntax — **set port** *port* **name** *name*

- *port* — Number of a physical port. You can specify only one port.
- **name** *name* — Alphanumeric string of up to 16 characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To simplify configuration and avoid confusion between a port's number and its name, 3Com recommends that you do not use numbers as port names.

Examples — The following command sets the name of port 7 to *adminpool*:

```
WX1200# set port 7 name adminpool
success: change accepted.
```

See Also

- **clear port name** on page 66
- **display port status** on page 73

set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

Syntax — **set port negotiation** *port-list* {**enable** | **disable**}

- *port-list* — List of physical ports. MSS disables or reenables autonegotiation on all the specified ports.
- **enable** — Enables autonegotiation on the specified ports.
- **disable** — Disables autonegotiation on the specified ports.

Defaults — Autonegotiation is enabled on all Ethernet ports by default.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — WX1200 10/100 Ethernet ports support half-duplex and full-duplex operation.

Examples — The following command disables autonegotiation on ports 3 and 5:

```
WX1200# set port negotiation 3,5 disable
```

The following command enables autonegotiation on port 2:

```
WX1200# set port negotiation 2 enable
```

set port poe

Enables or disables Power over Ethernet (PoE) on ports connected to MAP access points.

CAUTION: *When you set the port type for MAP use, you can enable PoE on the port. Use the WX switch's PoE to power 3Com MAP access points only. If you enable PoE on ports connected to other devices, damage can result.*

Syntax — **`set port poe`** *`port-list`* **`enable`** | **`disable`**

- *`port-list`* — List of physical ports. MSS disables or reenables PoE on all the specified ports.
- **`enable`** — Enables PoE on the specified ports.
- **`disable`** — Disables PoE on the specified ports.

Defaults — PoE is disabled on network and wired authentication ports. The state on MAP access point ports depends on whether you enabled or disabled PoE when setting the port type. See **set port type ap** on page 91.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the WX1200 switch.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command disables PoE on ports 4 and 5, which are connected to a MAP access point:

```
WX1200# set port poe 4,5 disable
If you are enabling power on these ports, they must be connected only to approved
PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y
```

The following command enables PoE on ports 4 and 5:

```
WX1200# set port poe 4,5 enable
If you are enabling power on these ports, they must be connected only to approved
PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y
```

See Also

- **set port type ap** on page 91
- **set port type wired-auth** on page 94

set port preference

Configures a gigabit Ethernet port on a WX4400 to use the RJ-45 (copper) interface, when available, as the active link instead of the fiber interface.

Syntax — **set port preference** *port-list* **rj45**

- *port-list* — List of physical ports. MSS sets the preference on all the specified ports.
- **rj45** — Prefers the copper interface.

Defaults — When both the copper and fiber interfaces of a gigabit Ethernet port are connected, the GBIC (fiber) interface is the active link. The RJ-45 (copper) link is unused.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the WX4400.

If you set the preference to RJ-45 (copper) on a port that already has an active fiber link, MSS immediately changes the link to the copper interface.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command sets the preference of port 2 on a WX4400 to RJ-45 (copper):

```
WX4400# set port preference 2 rj45
```

See Also

- **clear port preference** on page 67
- **display port preference** on page 72

set port speed

Changes the speed of a port.

Syntax — **set port speed** *port-list* {**10** | **100** | **1000** | **auto**}

- *port-list* — List of physical ports. MSS sets the port speed on all the specified ports.
- **10** — Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.
- **100** — Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.
- **1000** — Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.
- **auto** — Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

Defaults — All ports are set to auto.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the port speed on ports 1 and 3 through 4 to 10 Mbps and sets the operating mode to full-duplex:

```
WX1200# set port speed 1,3-4 10
```

Downloaded from www.Manualslib.com manuals search engine

set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

Syntax — **`set port trap`** *`port-list`* {**`enable`** | **`disable`**}

- *`port-list`* — List of physical ports.
- **`enable`** — Enables the Telnet server.
- **`disable`** — Disables the Telnet server.

Defaults — SNMP linkup and linkdown traps are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The **set port trap** command overrides the global setting of the **set snmp trap** command.

The **set port type** command does not affect the global trap information displayed by the **display snmp configuration** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **display snmp configuration** command still indicates that the traps are globally enabled.

Examples — The following command enables SNMP linkup and linkdown traps on ports 3 and 4:

```
WX1200# set port trap 3-4 enable
```

See Also

- **set ip snmp server** on page 169
- **set snmp community** on page 175

Downloaded from www.Manualslib.com manuals search engine

set port type ap

Configures an WX switch port for a MAP access point.

CAUTION: *When you set the port type for MAP use, you must specify the PoE state (enable or disable) of the port. Use the WX switch's PoE to power 3Com MAP access points only. If you enable PoE on a port connected to another device, physical damage to the device can result.*

Before configuring a port as a MAP access point port, you must use the ***set system countrycode*** *command to set the IEEE 802.11 country-specific regulations on the WX switch. See "set system countrycode" on page 56.*

For a MAP that is indirectly connected to the WX switch through an intermediate Layer 2 or Layer 3 network, use the ***set dap*** *command to configure a Distributed MAP.*

Before changing the port type from ***ap*** *to* ***wired-auth*** *or from* ***wired-auth*** *to* ***ap****, you must reset the port with the clear port type command.*

Syntax — **`set port type ap`** *`port-list`* **`model`** {**`ap2750`** | **`ap3750`**| **`ap7250`** | **`ap8250`** | **`ap8750`** | **`mp-52`** | **`mp-241`** | **`mp-252`** | **`mp-262`** | **`mp-341`** | **`mp-352`** | **`mp-372`** | **`mp-372-CN`** | **`mp-37-JP`** | **`mp-620`}** **`poe`** {**`enable`** | **`disable`**} [**`radiotype`** {**`11a`** | **`11b`** | **`11g`**}]

- *`port-list`* — List of physical ports.
- **`model`** {**`ap2750`** | **`ap3750`**| **`ap7250`** | **`ap8250`** | **`ap8750`** | **`mp-52`** | **`mp-241`** | **`mp-252`** | **`mp-262`** | **`mp-341`** | **`mp-352`** | **`mp-372`** | **`mp-372-CN`** | **`mp-37-JP`** | **`mp-620`}** — MAP access point model:
- **`poe enable`** | **`disable`** — Power over Ethernet (PoE) state.
- **`radiotype 11a`** | **`11b`** | **`11g`** — Radio type:
  - **`11a`** — 802.11a
  - **`11b`** — 802.11b
  - **`11g`** — 802.11g

This option does not apply to single-radio models.

Defaults — All WX ports are network ports by default.

Downloaded from www.Manualslib.com manuals search engine

MAP access point models AP2750, MP-241, and MP-341 have a single radio that can be configured for 802.11a or 802.11b/g. Other MAP models have two radios. On two-radio models, one radio is always 802.11a. The other radio is 802.11b/g, but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the **set system countrycode** command does not allow 802.11g, the default is 802.11b.

MAP radios configured for 802.11g also allow associations from 802.11b clients by default. To disable support for 802.11b associations, use the **set radio-profile 11g-only** command on the radio profile that contains the radio.

The radios in models MP-620 require external antennas, and model MP-262 requires an external antenna for the 802.11b/g radio. The following models have internal antennas but also have connectors for optional use of external antennas instead: AP2750, AP3750, AP7250, AP8250, AP8750, MP-372, MP-372-CN, and MP-372-JP. (Antenna support on a specific model is limited to the antennas certified for use with that model.) To specify the antenna model, use the **set {ap | dap} radio antennatype** command.

Access — Enabled.

History — Introduced in MSS Version 3.0. New values for model option added in Version 4.1:

- AP3750
- AP2750

Usage — You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. Table 18 lists the default settings that MSS applies when you set a port's type to **ap.**

Downloaded from www.Manualslib.com manuals search engine

Table 18 MAP Access Port Defaults

Port Parameter	Setting
VLAN membership	Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Uses authentication parameters configured for users.
Port groups	Not applicable
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	Not applicable

This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the WX1200 switch. To manage a MAP access point on a switch model that does not have 10/100 Ethernet ports, use the **set dap** command to configure a Distributed MAP connection on the switch.

Examples — The following command sets ports 1 through 3 and port 5 for MAP access point model AP2750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap2750 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP7250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap7250 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8250 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8750 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

Downloaded from www.Manualslib.com manuals search engine

The following command resets port 5 by clearing it:

```
WX1200# clear port type 5
This may disrupt currently authenticated users.
Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- **clear dap** on page 64
- **clear port type** on page 68
- **set {ap | dap} radio antennatype** on page 334
- **set dap** on page 81
- **set port type wired-auth** on page 94
- **set radio-profile 11g-only** on page 347
- **set system countrycode** on page 56

set port type wired-auth

Configures a WX switch port for a wired authentication user.

*Before changing the port type from **ap** to **wired-auth** or from **wired-auth** to **ap**, you must reset the port with the **clear port type** command.*

Syntax — **set port type wired-auth** *port-list* [**tag** *tag-list*] [**max-sessions** *num*] [**auth-fall-thru** {**last-resort** | **none** | **web-portal**}]

- *port-list* — List of physical ports.
- *tag-list* — One or more numbers between 1 and 4094 that subdivide a wired authentication port into virtual ports.
- *num* — Maximum number of simultaneous user sessions supported.
- **last-resort** — Automatically authenticates the user, without requiring a username and password.
- **none** — Denies authentication and prohibits the user from accessing the network over this port.
- **web-portal** — Serves the user a web page from the MX switch's nonvolatile storage for secure login to the network.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The default tag-list is null (no tag values). The default number of sessions is 1. The default fallthru authentication type is none.

Access — Enabled.

History—Introduced in MSS Version 3.0. Option for WebAAA fallthru authentication type changed from **web-auth** to **web-portal** in MSS Version 4.0.

Usage — You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. Table 19 lists the default settings that MSS applies when you set a port's type to **ap**.

Table 19 Wired Authentication Port Details

Port Parameter	Setting
VLAN membership	Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Uses authentication parameters configured for users.
Port groups	Not applicable
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	1 (one).
Fallthru authentication type	None

For 802.1X clients, wired authentication works only if the clients are directly attached to the wired authentication port, or are attached through a hub that does not block forwarding of packets from the client to the PAE group address (01:80:c2:00:00:03).

Wired authentication works in accordance with the 802.1X specification, which prohibits a client from sending traffic directly to an authenticator's MAC address until the client is authenticated. Instead of sending traffic to the authenticator's MAC address, the client sends packets to the PAE group address.

Downloaded from www.Manualslib.com manuals search engine

The 802.1X specification prohibits networking devices from forwarding PAE group address packets, because this would make it possible for multiple authenticators to acquire the same client.

For non-802.1X clients, who use MAC authentication, WebAAA, or last-resort authentication, wired authentication works if the clients are directly attached or indirectly attached.

Examples — The following command sets port 2 for a wired authentication user:

```
WX1200# set port type wired-auth 2
success: change accepted
```

The following command sets port 7 for a wired authentication user and specifies a maximum of three simultaneous user sessions:

```
WX1200# set port type wired-auth 7 max-sessions 3
success: change accepted
```

See Also

- **clear port type** on page 68
- **set port type ap** on page 91

Downloaded from www.Manualslib.com manuals search engine

5 VLAN COMMANDS

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a mobility domain.

Commands by usage

This chapter presents VLAN commands alphabetically. Use Table 20 to locate commands in this chapter based on their use.

Table 20 VLAN Commands by Usage

Type	Command
Creation	**set security l2-restrict** on page 114
Ports	**set vlan port** on page 117
	clear security 12-restrict on page 99
	display vlan config on page 111
Roaming and Tunnels	**display roaming station** on page 106
	display roaming vlan on page 108
	display security 12-restrict on page 109
Restriction of Client Layer 2 Forwarding	**set security l2-restrict** on page 114
	display security 12-restrict on page 109
	clear security 12-restrict on page 99
	clear security 12-restrict counters on page 100
Tunnel Affinity	**set vlan tunnel-affinity** on page 118
FDB Entries	**set fdb** on page 113
	display fdb on page 102
	display fdb count on page 105
	clear fdb on page 98
FDB Aging Timeout	**set fdb agingtime** on page 114
	display fdb agingtime on page 104

Downloaded from www.Manualslib.com manuals search engine

clear fdb

Deletes an entry from the forwarding database (FDB).

Syntax — **clear fdb** {**perm** | **static** | **dynamic** | **port** *port-list*} [**vlan** *vlan-id*] [**tag** *tag-value*]

- **perm** — Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **static** — Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **dynamic** — Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option.
- **port** *port-list* — Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option.
- **vlan** *vlan-id* — VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed.
- **tag** *tag-value* — VLAN tag value that identifies a virtual port. If you do not specify a tag value, MSS deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interfaces

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

Examples — The following command clears all static forwarding database entries that match VLAN *blue*:

```
WX4400# clear fdb static vlan blue
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

The following command clears all dynamic forwarding database entries that match all VLANs:

```
WX4400# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 3 and 5:

```
WX4400# clear fdb port 3,5
success: change accepted.
```

See Also

- **display fdb** on page 102
- **set fdb** on page 113

clear security 12-restrict

Removes one or more MAC addresses from the list of destination MAC addresses to which clients in a VLAN are allowed to send traffic at Layer 2.

Syntax — **clear security 12-restrict vlan** *vlan-id* [**permit-mac** *mac-addr* [*mac-addr*]|**all**]

- *vlan-id* — VLAN name or number.
- **permit-mac** *mac-addr* [*mac-addr*] — List of MAC addresses. MSS no longer allows clients in the VLAN to send traffic to the MAC addresses at Layer 2.
- **all** — Removes all MAC addresses from the list.

Defaults — If you do not specify a list of MAC addresses or **all**, all addresses are removed.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN will be able to communicate directly.

To clear the statistics counters without removing any MAC addresses, use the **clear security l2-restrict counters** command instead.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses to which clients in VLAN *abc_air* are allowed to send traffic at Layer 2:

```
WX4400# clear security 12-restrict vlan abc_air permit-mac
aa:bb:cc:dd:ee:ff
success: change accepted.
```

See Also

- **clear security 12-restrict counters** on page 100
- **clear security 12-restrict** on page 99
- **display security 12-restrict** on page 109

clear security 12-restrict counters

Clears statistics counters for Layer 2 forwarding restriction.

Syntax — **clear security 12-restrict counters [vlan** *vlan-id* | **all]**

- *vlan-id* — VLAN name or number.
- **all** — Clears Layer 2 forwarding restriction counters for all VLANs.

Defaults — If you do not specify a VLAN or **all**, counters for all VLANs are cleared.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — To clear MAC addresses from the list of addresses to which clients are allowed to send data, use the **clear security 12-restrict** command instead.

Examples — The following command clears Layer 2 forwarding restriction statistics for VLAN *abc_air*:

```
WX4400# clear security 12-restrict counters vlan abc_air
success: change accepted.
```

See Also

- **clear security 12-restrict** on page 99
- **set security l2-restrict** on page 114
- **display security 12-restrict** on page 109

Downloaded from www.Manualslib.com manuals search engine

clear vlan

Removes physical or virtual ports from a VLAN or removes a VLAN entirely.

CAUTION: *When you remove a VLAN, MSS completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.*

Syntax — **`clear vlan`** *`vlan-id`* [**`port`** *`port-list`* [**`tag`** *`tag-value`*]]

- *`vlan-id`* — VLAN name or number.
- **port** *`port-list`* — List of physical ports. MSS removes the specified ports from the VLAN. If you do not specify a list of ports, MSS removes the VLAN entirely.
- **tag** *`tag-value`* — Tag number that identifies a virtual port. MSS removes only the specified virtual port from the specified physical ports.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you do not specify a *port-list*, the entire VLAN is removed from the configuration.

You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the ***port*** port-list *option.*

Examples — The following command removes port 1 from VLAN *green*:

```
WX4400# clear vlan green port 1
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command removes port 4, which uses tag value 69, from VLAN *red*:

```
WX1200# clear vlan red port 4 tag 69
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

The following command completely removes VLAN *marigold*:

```
WX4400# clear vlan marigold
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

See Also

- **set vlan port** on page 117
- **display vlan config** on page 111

display fdb

Displays entries in the forwarding database.

Syntax — **display fdb** [*mac-addr-glob* [**vlan** *vlan-id*]] **display fdb** {**perm** | **static** | **dynamic** | **system** | **all**} [**port** *port-list* | **vlan** *vlan-id*]

- *mac-addr-glob* — A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*****) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)
- **vlan** *vlan-id* — Name or number of a VLAN for which to display entries.
- **perm** — Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- **dynamic** — Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
- **system** — Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users.
- **all** — Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.
- **port** *port-list* — Destination port(s) for which to display entries.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — All.

History —Introduced in MSS Version 3.0.

Usage — To display the entire forwarding database, enter the **display fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

Examples — The following command displays all entries in the forwarding database:

```
WX4400# display fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      aa:bb:cc:dd:ee:ff      *       3                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
WX4400# display fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 2
```

Table 21 describes the fields in the **display fdb** output.

Table 21 Output for display fdb

Field	Description
VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of this forwarding entry's destination.

Downloaded from www.Manualslib.com manuals search engine

Table 21 Output for display fdb (continued)

Field	Description
CoS	Type of entry. The entry types are explained in the first row of the command output. **Note:** This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.
Destination Ports	Wireless LAN switch port associated with the entry. A WX switch sends traffic to the destination MAC address through this port.
Protocol Type	Layer 3 protocol address types that can be mapped to this entry.
Total Matching FDB Entries Displayed	Number of entries displayed by the command.

See Also

- **clear fdb** on page 98
- **set fdb** on page 113

display fdb agingtime

Displays the aging timeout period for forwarding database entries.

Syntax — **`display fdb agingtime`** [**`vlan`** `vlan-id`]

- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays the aging timeout period for all VLANs:

```
WX1200# display fdb agingtime
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set fdb agingtime** on page 114

display fdb count

Lists the number of entries in the forwarding database.

Syntax — **`display fdb count`** {**`perm`** | **`static`** | **`dynamic`**} [**`vlan`** *`vlan-id`*]

- **`perm`** — Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **`static`** — Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- **`dynamic`** — Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
- **`vlan`** *`vlan-id`* — VLAN name or number. Entries are listed for only the specified VLAN.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

The following command lists the number of dynamic entries that the forwarding database contains:

```
WX1200# display fdb count dynamic
Total Matching Entries = 2
```

See Also

- **display fdb** on page 102

Downloaded from www.Manualslib.com manuals search engine

display roaming station

Shows a list of the stations roaming to the wireless LAN switch through a VLAN tunnel.

Syntax — **display roaming station** [**vlan** *vlan-id*] [**peer** *ip-addr*]

- **vlan** *vlan-id* — Output is restricted to stations using this VLAN.
- **peer** *ip-addr* — Output is restricted to stations tunnelling through this peer WX switch in the Mobility Domain.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Old AP MAC field removed in MSS Version 4.1.

Usage — The output displays roaming stations within the previous 1 second.

Examples — To display all stations roaming to the WX switch, type the following command:

```
WX4400# display roaming station
User Name                Station Address         VLAN            State
------------------------ --------------- ----------------- -------------- ------
redsqa                   10.10.10.5              violet          Up
```

Table 22 describes the fields in the display.

Table 22 Output for display roaming station

Field	Description
User Name	Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on a wireless LAN switch.
Station Address	IP address of the user device.
VLAN	Name of the VLAN to which the RADIUS server or WX switch local user database assigned the user.

Downloaded from www.Manualslib.com manuals search engine

Table 22 Output for display roaming station (continued)

Field	Description
State	State of the session: ▪ **Setup** — Station is attempting to roam to this WX switch. This switch has asked the WX from which the station is roaming for the station's session information and is waiting for a reply. ▪ **Up** — MSS has established a tunnel between the WX switches and the station has successfully roamed to this WX over the tunnel. ▪ **Chck** — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to the peer switch. ▪ **TChck** — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to this switch. ▪ **WInd** — This WX switch is waiting for network congestion to clear before sending the roaming indication to the roaming peer WX switch. ▪ **WResp** — This WX switch is waiting for network congestion to clear before sending the roaming response to the roaming peer WX switch.

See Also

- **display roaming vlan** on page 108

Downloaded from www.Manualslib.com manuals search engine

display roaming vlan

Shows all VLANs in the mobility domain, the WX switches servicing the VLANs, and their tunnel affinity values configured on each switch for the VLANs.

Syntax — **`display roaming vlan`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command shows the current roaming VLANs:

```
WX4400# display roaming vlan
VLAN             WX              Affinity
---------------- --------------- --------
vlan-cs          192.168.14.2           5
vlan-eng         192.168.14.4           5
vlan-fin         192.168.14.2           5
vlan-it          192.168.14.4           5
vlan-it          192.168.14.2           5
vlan-pm          192.168.14.2           5
vlan-sm          192.168.14.2           5
vlan-tp          192.168.14.4           5
vlan-tp          192.168.14.2           5
```

Table 23 describes the fields in the display.

Table 23 Output for display roaming vlan

Field	Description
VLAN	VLAN name.
WX	System IP address of the wireless LAN switch on which the VLAN is configured.
Affinity	Preference of this WX switch for forwarding user traffic for the VLAN. A higher number indicates a greater preference.

See Also

- **display roaming station** on page 106
- **display vlan config** on page 111

Downloaded from www.Manualslib.com manuals search engine

display security 12-restrict

Displays configuration information and statistics for Layer 2 forwarding restriction.

Syntax — **`display security 12-restrict [vlan`** *`vlan-id`* **|** **`all]`**

`vlan-id` — VLAN name or number.

`all` — Displays information for all VLANs.

Defaults — If you do not specify a VLAN name or **all**, information is displayed for all VLANs.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command shows Layer 2 forwarding restriction information for all VLANs:

```
VLAN Name          En Drops      Permit MAC          Hits
---- ----------- -- ---------- ------------------ ----------
   1 default       Y          0 00:0b:0e:02:53:3e        5947
                             00:30:b6:3e:5c:a8            9
   2 vlan-2        Y          0 04:04:04:04:04:04          0
```

Table 24 describes the fields in the display.

Table 24 Output for display security 12-restrict

Field	Description
VLAN	VLAN number.
Name	VLAN name.
En	Enabled state of the feature for the VLAN: ▪ Y — Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC. ▪ N — Disabled. Layer 2 forwarding is not restricted.
Drops	Number of packets dropped because the destination MAC address was not one of the addresses listed under Permit MAC.
Permit MAC	MAC addresses to which clients in the VLAN are allowed to send traffic at Layer 2.

Downloaded from www.Manualslib.com manuals search engine

Table 24 Output for display security 12-restrict

Field	Description
Hits	Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC.

See Also

- **clear security 12-restrict** on page 99
- **clear security 12-restrict counters** on page 100
- **set security l2-restrict** on page 114

display tunnel

Shows the tunnels from the wireless LAN switch where you type the command.

Syntax — **`display tunnel`**

Defaults — None.

Access — Enabled

History —Introduced in MSS Version 3.0.

Examples — To display all tunnels from a WX switch to other WX switches in the Mobility Domain, type the following command.

```
WX4400# display tunnel
VLAN            Local Address   Remote Address  State   Port  LVID  RVID
--------------- --------------- --------------- ------- ----- ----- -----
vlan-eng        192.168.14.2    192.168.14.4    DORMANT  1024  4096   130
```

Table 25 describes the fields in the display.

Table 25 Output for display tunnel

Field	Description
VLAN	VLAN name.
Local Address	IP address of the local end of the tunnel. This is the system IP address of the wireless access switch where you enter the command.

Downloaded from www.Manualslib.com manuals search engine

Table 25 Output for display tunnel (continued)

Field	Description
Remote Address	IP address of the remote end of the tunnel. This is the system IP address of another WX switch in the mobility domain.
State	Tunnel state: ▪ Up ▪ Dormant
Port	Tunnel port ID.
LVID	Local VLAN ID.
RVID	Remote VLAN ID.

See Also

- **display vlan config** on page 111

display vlan config

Shows VLAN information.

Syntax — **`display vlan config`** [*`vlan-id`*]

- *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays information for VLAN *burgundy*:

```
WX1200# display vlan config burgundy
                       Admin  VLAN  Tunl                          Port
VLAN Name              Status State Affin Port              Tag   State
---- ----------------- ------ ----- ----- ----------------- ----- -----
   2 burgundy          Up     Up        5
                                          2                  none Up
                                          3                  none Up
                                          4                  none Up
                                          6                  none Up
4094 web-aaa           Up     Up        0
                                          2                  4094 Up
                                          t:10.10.40.4       none Up
```

Downloaded from www.Manualslib.com manuals search engine

Table 26 describes the fields in this display.

Table 26 Output for display vlan config

Field	Description
VLAN	VLAN number.
Name	VLAN name.
Admin Status	Administrative status of the VLAN: ▪ **Down** — The VLAN is disabled. ▪ **Up** — The VLAN is enabled.
VLAN State	Link status of the VLAN: ▪ **Down** — The VLAN is not connected. ▪ **Up** — The VLAN is connected.
Tunl Affin	Tunnel affinity value assigned to the VLAN.
Port	Member port of the VLAN. The port can be a physical port or a virtual port. ▪ Physical ports are 10/100 Ethernet or gigabit Ethernet ports on the WX switch, and are listed by port number. ▪ Virtual ports are tunnels to other WX switches in a mobility domain, and are listed as follows: t:*ip-addr*, where *ip-addr* is the system IP address of the WX switch at the other end of the tunnel. **Note:** This field can include MAP access ports and wired authentication ports, because MSS dynamically adds these ports to a VLAN when handling user traffic for the VLAN.
Tag	Tag value assigned to the port.
Port State	Link state of the port: ▪ **Down** — The port is not connected. ▪ **Up** — The port is connected.

See Also

- **clear security 12-restrict** on page 99
- **set security l2-restrict** on page 114
- **set vlan port** on page 117
- **set vlan tunnel-affinity** on page 118

Downloaded from www.Manualslib.com manuals search engine

set fdb

Adds a permanent or static entry to the forwarding database.

Syntax — **set fdb** {**perm** | **static**} *mac-addr* **port** *port-list* **vlan** *vlan-id* [**tag** *tag-value*]

- **perm** — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- *mac-addr* — Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-list* — List of physical destination ports for which to add the entry. A separate entry is added for each port you specify.
- **vlan** *vlan-id* — Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.
- **tag** *tag-value* — VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4095. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Examples — The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN *blue*:

```
WX1200# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.
```

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the *default* VLAN:

```
WX4400# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear fdb** on page 98
- **display fdb** on page 102

set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

Syntax — **set fdb agingtime** *vlan-id* **age** *seconds*

- *vlan-id* — VLAN name or number. The timeout period change applies only to entries that match the specified VLAN.
- **age** *seconds* — Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled.

Defaults — The aging timeout period is 300 seconds (5 minutes).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the aging timeout period to 600 seconds for entries that match VLAN *orange*:

```
WX4400# set fdb agingtime orange age 600
success: change accepted.
```

See Also

- **display fdb agingtime** on page 104

set security l2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN's gateway routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified gateway routers.

Syntax — **set security l2-restrict vlan** *vlan-id* [**mode** {**enable** | **disable**}] [**permit-mac** *mac-addr* [*mac-addr*]]

- *vlan-id* — VLAN name or number.

Downloaded from www.Manualslib.com manuals search engine

- **mode** — Enables or disables restriction of Layer 2 forwarding. **{enable | disable}**
- **permit-mac *mac-addr*** [***mac-addr***] — MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses.

Defaults — Layer 2 restriction is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security 12-restrict** command to remove it, then use the **set security 12-restrict** command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the **mode enable** option with this command

Examples — The following command restricts Layer 2 forwarding of client data in VLAN *abc_air* to the gateway routers with MAC address aa:bb:cc:dd:ee:ff and 11:22:33:44:55:66:

```
WX4400# set security 12-restrict vlan abc_air mode enable
permit-mac aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
success: change accepted.
```

See Also

- **clear security 12-restrict** on page 99
- **clear security 12-restrict counters** on page 100
- **display security 12-restrict** on page 109

Downloaded from www.Manualslib.com manuals search engine

set vlan name

Creates a VLAN and assigns a number and name to it.

Syntax — **`set vlan`** *`vlan-num`* **`name`** *`name`*

- *`vlan-num`* — VLAN number. You can specify a number from 2 through 4093.
- *`name`* — String up to 16 alphabetic characters long.

Defaults — VLAN 1 is named *default* by default. No other VLANs have default names.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

3Com recommends that you do not use the name *default*. This name is already used for VLAN 1. 3Com also recommends that you do not rename the default VLAN.

You cannot use a number as the first character in a VLAN name. 3Com recommends that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names *red* and *RED*.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a wireless LAN switch. If the WX switch is not configured with the VLAN the client is on, but is configured with a VLAN that has the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN *red* but the WX switch to which the client roams has VLAN *RED* instead, RADIUS authorization fails.

Examples — The following command assigns the name *marigold* to VLAN 3:

```
WX4400# set vlan 3 name marigold
success: change accepted.
```

See Also

- **set vlan port** on page 117

Downloaded from www.Manualslib.com manuals search engine

set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

Syntax — **set vlan** *vlan-id* **port** *port-list* [**tag** *tag-value*]

- *vlan-id* — VLAN name or number.
- **port** *port-list* — List of physical ports.
- **tag** *tag-value* — Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

By default, no ports are members of any VLANs. A wireless LAN switch cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can combine this command with the **set port name** command to assign the name and add the ports at the same time.

If you do not specify a tag value, the WX switch sends untagged frames for the VLAN. If you do specify a tag value, the WX sends tagged frames only for the VLAN.

If you do specify a tag value, 3Com recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but some other switches do.

Examples — The following command assigns the name *beige* to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
WX1200# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 6 to VLAN *beige* and assigns tag value 86 to the port:

```
WX1200# set vlan beige port 6 tag 86
success: change accepted.
```

See Also

- **clear security 12-restrict** on page 99
- **display vlan config** on page 111
- **set security l2-restrict** on page 114

Downloaded from www.Manualslib.com manuals search engine

set vlan tunnel-affinity

Changes a wireless LAN switch's preferability within a mobility domain for tunneling user traffic for a VLAN. When a user roams to a WX switch that is not a member of the user's VLAN, the WX can forward the user traffic by tunneling to another WX switch that is a member of the VLAN.

Syntax — **`set vlan`** *`vlan-id`* **`tunnel-affinity`** *`num`*

- *`vlan-id`* — VLAN name or number.
- *`num`* — Preference of this switch for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults — Each VLAN on a WX switch's network ports has an affinity value of 5 by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Increasing a WX switch's affinity value increases the WX's preferability for forwarding user traffic for the VLAN.

If more than one WX switch has the highest affinity value, MSS randomly selects one of the WX switches for the tunnel.

Examples — The following command changes the VLAN affinity for VLAN *beige* to 10:

```
WX4400# set vlan beige tunnel-affinity 10
success: change accepted.
```

See Also

- **display roaming vlan** on page 108
- **display vlan config** on page 111

Downloaded from www.Manualslib.com manuals search engine

6 Quality of Service Commands

Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that WX switches and MAP access points give preferential treatment to high-priority traffic such as voice and video.

(To override the prioritization for specific traffic, use access controls lists [ACLs] to set the Class of Service [CoS] for the packets. See "Security ACL Commands" on page 445.)

Commands by Usage

This chapter presents QOS commands alphabetically. Use Table 27 to locate commands in this chapter based on their use.

Table 27 QOS Commands by Usage

Type	Command
QOS Settings	**display qos** on page 123
	display qos dscp-table on page 124
	set qos cos-to-dscp-map on page 121
	set qos dscp-to-cos-map on page 122
	clear qos on page 120

Downloaded from www.Manualslib.com manuals search engine

clear qos

Resets the switch's mapping of Differentiated Services Code Point (DSCP) values to internal QoS values.

The switch's internal QoS map ensures that prioritized traffic remains prioritized while transiting through the WX switch. A WX switch uses the QoS map to do the following:

- Classify inbound packets by mapping their DSCP values to one of eight internal QoS values
- Classify outbound packets by marking their DSCP values based on the switch's internal QoS values

Syntax — **clear qos [cos-to-dscp-map [***from-qos***] | dscp-to-cos-map [***from-dscp***]]**

- **cos-to-dscp-map** — Resets the mapping between the specified internal QoS value and the DSCP values with which MSS marks outbound packets. QoS values are from 0 to 7.
- **dscp-to-cos-map** — Resets the mapping between the specified range of DSCP values and internal QoS value with which MSS classifies inbound packets.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — To reset all mappings to their default values, use the **clear qos** command without the optional parameters.

Examples — The following command resets all QoS mappings:

```
WX1200# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
WX1200# clear qos dscp-to-qos-map 44
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

set qos cos-to-dscp-map

Changes the value to which MSS maps an internal QoS value when marking outbound packets.

Syntax — **`set qos cos-to-dscp-map`** *`level`* **`dscp`** *`dscp-value`*

- *`level`* — Internal CoS value. You can specify a number from 0 to 7.
- **`dscp`** *`dscp-value`* — DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

Defaults — The defaults are listed by the **display qos** command.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command maps internal CoS value 5 to DSCP value 50:

```
WX1200# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be
classified as cos 6
```

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets that receive CoS 5 upon ingress will be marked with a DSCP value equivalent to CoS 6 upon egress.

See Also

- **set qos dscp-to-cos-map** on page 122
- **display qos** on page 123

Downloaded from www.Manualslib.com manuals search engine

set qos dscp-to-cos-map

Changes the internal QoS value to which MSS maps a packet's DSCP value when classifying inbound packets.

Syntax — `set qos dscp-to-cos-map` *`dscp-range`* `cos` *`level`*

- *`dscp-range`* — You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.
- **`cos`** *`level`* — Internal QoS value. You can specify a number from 0 to 7.

Defaults — The defaults are listed by the **display qos** command.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command maps DSCP values 40-56 to internal CoS value 6:

```
WX1200# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be
classified as cos 7
warning: cos 7 is marked with dscp 56 which will be
classified as cos 6
```

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

See Also

- **set qos cos-to-dscp-map** on page 121
- **display qos** on page 123

Downloaded from www.Manualslib.com manuals search engine

display qos

Displays the switch's QoS settings.

Syntax — `display qos [default]`

- `default` — Displays the default mappings.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command displays the default QoS settings:

```
WX1200# display qos default

Ingress QoS Classification Map (dscp-to-cos)

Ingress DSCP        CoS Level
============================================================
       00-09       0    0    0    0    0      0    0    0    1
1
       10-19       1    1    1    1    1      1    2    2    2
2
       20-29       2    2    2    2    3      3    3    3    3
3
       30-39       3    3    4    4    4      4    4    4    4
4
       40-49       5    5    5    5    5      5    5    5    6
6
       50-59       6    6    6    6    6      6    7    7    7
7
        60-63        7    7    7    7


Egress QoS Marking Map (cos-to-dscp)

CoS Level              0      1      2      3      4      5
6      7
============================================================
Egress DSCP             0      8     16     24     32     40
48     56
Egress ToS byte      0x00   0x20   0x40   0x60   0x80   0xA0
0xC0   0xE0
```

See Also

- **display qos dscp-table** on page 124

Downloaded from www.Manualslib.com manuals search engine

display qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

Syntax — `display qos dscp-table`

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0 as the **display security acl dscp** command and renamed in MSS Version 4.1.

Examples — The following command displays the table:

```
WX1200# display qos dscp-table

DSCP           TOS            precedence    tos
dec  hex       dec  hex
-----------------------------------------------
  0  0x00        0  0x00               0      0
  1  0x01        4  0x04               0      2
  2  0x02        8  0x08               0      4
...
 63  0x3f      252  0xfc               7     14
```

See Also

- **display qos** on page 123

Downloaded from www.Manualslib.com manuals search engine

7 IP Services Commands

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), and aliases, and to ping a host or trace a route.

Commands by Usage

This chapter presents IP services commands alphabetically. Use Table 28 to locate the commands in this chapter based on their use.

Table 28 IP Services Commands by Usage

Type	Command
IP Interface	**set interface** on page 160
	set interface dhcp-client on page 161
	set interface status on page 163
	display interface on page 142
	display dhcp-client on page 138
	clear interface on page 127
System IP Address	**set system ip-address** on page 192
	clear system ip-address on page 136
IP Route	**set ip route** on page 167
	display ip route on page 146
	clear ip route on page 130
SSH Management	**set ip ssh server** on page 171
	set ip ssh on page 170
Telnet Management	**set ip telnet** on page 171
	set ip telnet server on page 172
	display ip telnet on page 148
	clear ip telnet on page 131

Downloaded from www.Manualslib.com manuals search engine

Table 28 IP Services Commands by Usage (continued)

Type	Command
HTTPS Management	**set ip https server** on page 167
	display ip https on page 145
DNS	**set ip dns** on page 164
	set ip dns domain on page 165
	set ip dns server on page 166
	display ip dns on page 144
	clear ip dns domain on page 129
	clear ip dns server on page 129
IP Alias	**set ip alias** on page 164
	display ip alias on page 143
	clear ip alias on page 128
Time and Date	**set timedate** on page 193
	set timezone on page 194
	set summertime on page 191
	display timedate on page 155
	display timezone on page 155
	display summertime on page 154
	clear timezone on page 136
	clear summertime on page 135
NTP	**set ntp** on page 173
	set ntp server on page 174
	set ntp update-interval on page 175
	display ntp on page 149
	clear ntp server on page 131
	clear ntp update-interval on page 132
ARP	**set arp** on page 158
	set arp agingtime on page 159
	display dhcp-client on page 138
SNMP	**set snmp protocol** on page 186
	set snmp security on page 187
	set snmp community on page 175
	set snmp usm on page 188

Downloaded from www.Manualslib.com manuals search engine

Table 28 IP Services Commands by Usage (continued)

Type	Command
	set snmp notify profile on page 177
	set snmp notify target on page 181
	set ip snmp server on page 169
	display snmp status on page 153
	display snmp community on page 151
	display snmp usm on page 154
	display snmp notify profile on page 152
	display snmp notify target on page 152
	display snmp counters on page 152
	clear snmp community on page 133
	clear snmp usm on page 134
	clear snmp notify profile on page 133
	clear snmp notify target on page 134
Ping	**ping** on page 156
Telnet Client	**telnet** on page 195
Traceroute	**traceroute** on page 197
DHCP server	**set interface dhcp-server** on page 162
	display dhcp-server on page 140

clear interface

Removes an IP interface.

Syntax — **`clear interface`** *`vlan-id`* **`ip`**

- *`vlan-id`* — VLAN name or number

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations

Downloaded from www.Manualslib.com manuals search engine

- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — The following command removes the IP interface configured on VLAN *mauve*:

```
WX1200# clear interface mauve ip
success: cleared ip on vlan mauve
```

See Also

- **set interface** on page 160
- **set interface dhcp-client** on page 161
- **display interface** on page 142

clear ip alias

Removes an alias, which is a string that represents an IP address.

Syntax — **clear ip alias** *name*

name — Alias name

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the alias server1:

```
WX1200# clear ip alias server1
success: change accepted.
```

See Also

- **display ip alias** on page 143

Downloaded from www.Manualslib.com manuals search engine

clear ip dns domain

Removes the default DNS domain name.

Syntax — **`clear ip dns domain`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the default DNS domain name from a WX switch:

```
WX1200# clear ip dns domain
Default DNS domain name cleared.
```

See Also

- **clear ip dns server** on page 129
- **display ip dns** on page 144
- **set ip dns** on page 164
- **set ip dns domain** on page 165
- **set ip dns server** on page 166

clear ip dns server

Removes a DNS server from a WX switch configuration.

Syntax — **`clear ip dns server`** *`ip-addr`*

- *`ip-addr`* — IP address of a DNS server.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes DNS server 10.10.10.69 from a WX switch's configuration:

```
WX4400# clear ip dns server 10.10.10.69
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear ip dns domain** on page 129
- **display ip dns** on page 144
- **set ip dns** on page 164
- **set ip dns domain** on page 165
- **set ip dns server** on page 166

clear ip route

Removes a route from the IP route table.

Syntax — **`clear ip route`** {**`default`** | *`ip-addr mask`* | *`ip-addr/mask-length`*} **`gateway`**

- *`default`* — Default route.

***default** is an alias for IP address 0.0.0.0/0.*

- *`ip-addr mask`* — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *`ip-addr/mask-length`* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
- *`gateway`* — IP address, DNS hostname, or alias of the next-hop router.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the route to destination 10.10.10.68/24 through gateway router 10.10.10.1:

```
WX1200# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

See Also

- **display ip route** on page 146
- **set ip route** on page 167

Downloaded from www.Manualslib.com manuals search engine

clear ip telnet

Resets the Telnet server's TCP port number to its default value. A WX switch listens for Telnet management traffic on the Telnet server port.

Syntax — **`clear ip telnet`**

Defaults — The default Telnet port number is 23.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command resets the TCP port number for Telnet management traffic to its default:

```
WX4400# clear ip telnet
success: change accepted.
```

See Also

- **display ip https** on page 145
- **display ip telnet** on page 148
- **set ip https server** on page 167
- **set ip telnet** on page 171
- **set ip telnet server** on page 172

clear ntp server

Removes an NTP server from a WX switch configuration.

Syntax — **`clear ntp server`** {*ip-addr* | **`all`**}

- *ip-addr* — IP address of the server to remove, in dotted decimal notation.
- **`all`** — Removes all NTP servers from the configuration.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command removes NTP server 192.168.40.240 from a WX switch configuration:

```
WX4400# clear ntp server 192.168.40.240
success: change accepted.
```

See Also

- **clear ntp update-interval** on page 132
- **display ntp** on page 149
- **set ntp** on page 173
- **set ntp server** on page 174
- **set ntp update-interval** on page 175

clear ntp update-interval

Resets the NTP update interval to the default value.

Syntax — **clear ntp update-interval**

Defaults — The default NTP update interval is 64 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the NTP interval to the default value, type the following command:

```
WX4400# clear ntp update-interval
success: change accepted.
```

See Also

- **clear ntp server** on page 131
- **display ntp** on page 149
- **set ntp** on page 173
- **set ntp server** on page 174
- **set ntp update-interval** on page 175

Downloaded from www.Manualslib.com manuals search engine

clear snmp community

Clears an SNMP community string.

Syntax — **`clear snmp community name`** *`comm-string`*

- *`comm-string`* — Name of the SNMP community you want to clear.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command clears community string *setswitch2*:

```
WX1200# clear snmp community name setswitch2
success: change accepted.
```

See Also

- **set snmp community** on page 175
- **display snmp community** on page 151

clear snmp notify profile

Clears an SNMP notification profile.

Syntax — **`clear snmp notify profile`** *`profile-name`*

- *`profile-name`* — Name of the notification profile you are clearing.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command clears notification profile *snmpprof_rfdetect*:

```
WX1200# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set snmp notify profile** on page 177
- **display snmp notify profile** on page 152

clear snmp notify target

Clears an SNMP notification target.

Syntax — **clear snmp notify target** *target-num*

- *target-num* — ID of the target.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command clears notification target 3:

```
WX1200# clear snmp notify target 3
success: change accepted.
```

See Also

- **set snmp notify target** on page 181
- **display snmp notify target** on page 152

clear snmp usm

Clears an SNMPv3 user.

Syntax — **clear snmp usm** *usm-username*

- *usm-username* — Name of the SNMPv3 user you want to clear.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command clears SNMPv3 user *snmpmgr1*:

```
WX1200# clear snmp usm snmpmgr1
success: change accepted.
```

See Also

- **set snmp usm** on page 188
- **display snmp usm** on page 154

clear summertime

Clears the summertime setting from a wireless LAN switch.

Syntax — **clear summertime**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear the summertime setting from a WX switch, type the following command:

```
WX1200# clear summertime
success: change accepted.
```

See Also

- **clear timezone** on page 136
- **display summertime** on page 154
- **display timedate** on page 155
- **display timezone** on page 155
- **set summertime** on page 191
- **set timedate** on page 193
- **set timezone** on page 194

Downloaded from www.Manualslib.com manuals search engine

clear system ip-address

Clears the system IP address.

CAUTION: *Clearing the system IP address disrupts the system tasks that use the address.*

Syntax — **`clear system ip-address`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — To clear the system IP address, type the following command:

```
WX1200# clear system ip-address
success: change accepted.
```

See Also

- **display system** on page 43
- **set system ip-address** on page 192

clear timezone

Clears the time offset for the wireless LAN switch's real-time clock from Coordinated Universal Time (UTC). UTC is also know as Greenwich Mean Time (GMT).

Syntax — **`clear timezone`**

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History — Introduced in MSS Version 3.0.

Examples — To return the WX switch's real-time clock to UTC, type the following command:

```
WX4400# clear timezone
success: change accepted.
```

See Also

- **clear summertime** on page 135
- **set summertime** on page 191
- **set timedate** on page 193
- **set timezone** on page 194
- **display summertime** on page 154
- **display timedate** on page 155
- **display timezone** on page 155

display arp

Shows the ARP table.

Syntax — **display arp** [*ip-addr*]

- *ip-addr* — IP address.

Defaults — If you do not specify an IP address, the whole ARP table is displayed.

Usage — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays ARP entries:

```
WX4400# display arp
ARP aging time: 1200 seconds

Host                          HW Address        VLAN  Type    State
----------------------------- ----------------- ----- ------- --------
10.5.4.51                     00:0b:0e:02:76:f5     1 DYNAMIC RESOLVED
10.5.4.53                     00:0b:0e:02:76:f7     1 LOCAL   RESOLVED
```

Downloaded from www.Manualslib.com manuals search engine

Table 29 describes the fields in this display.

Table 29 Output for display arp

Field	Description
ARP aging time	Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table.
Host	IP address, hostname, or alias.
HW Address	MAC address mapped to the IP address, hostname, or alias.
VLAN	VLAN the entry is for.
Type	Entry type: ▪ **DYNAMIC** — Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout. ▪ **LOCAL** — Entry for the WX switch's MAC address. Each VLAN has one local entry for the WX switch's MAC address. ▪ **PERMANENT** — Entry does not age out and remains in the configuration even following a reboot. ▪ **STATIC** — Entry does not age out but is removed after a reboot.
State	Entry state: ▪ **RESOLVING** — MSS sent an ARP request for the entry and is waiting for the reply. ▪ **RESOLVED** — Entry is resolved.

See Also

- **set arp** on page 158
- **set arp agingtime** on page 159

display dhcp-client

Displays DHCP client information for all VLANs.

Syntax — **`display dhcp-client`**

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays DHCP client information:

```
WX1200# display dhcp-client
 Interface:            corpvlan(4)
 Configuration Status: Enabled
 DHCP State:           IF_UP
 Lease Allocation:     65535 seconds
 Lease Remaining:      65532 seconds
 IP Address:           10.3.1.110
 Subnet Mask:          255.255.255.0
 Default Gateway:      10.3.1.1
 DHCP Server:          10.3.1.4
 DNS Servers:          10.3.1.29
 DNS Domain Name:      mycorp.com
```

Table 30 describes the fields in this display.

Table 30 Output for display dhcp-client

Field	Description
Interface	VLAN name and number.
Configuration Status	Status of the DHCP client on this VLAN: ■ Enabled ■ Disabled
DHCP State	State of the IP interface: ■ IF_UP ■ IF_DOWN
Lease Allocation	Duration of the address lease.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address received from the DHCP server
Subnet Mask	Network mask of the IP address received from the DHCP server.
Default Gateway	Default gateway IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address.
DHCP Server	IP address of the DHCP server.
DNS Servers	DNS server IP address(es) received from the DHCP server.
DNS Domain Name	Default DNS domain name received from the DHCP server.

See Also

- **set interface dhcp-client** on page 161

Downloaded from www.Manualslib.com manuals search engine

display dhcp-server

Displays MSS DHCP server information.

Syntax — **`display dhcp-server [interface`** *`vlan-id`*`] [verbose]`

- **`interface`** *`vlan-id`* — Displays the IP addresses leased by the specified VLAN.
- **`verbose`**— Displays configuration and status information for the MSS DHCP server.

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Examples — The following command displays the addresses leased by the MSS DHCP server:

```
WX1200# display dhcp-server
VLAN Name   Address      MAC            Lease Remaining (sec)
----------  --------   ----------- ------------------------
1 default   10.10.20.2  00:01:02:03:04:05   12345
1 default   10.10.20.3  00:01:03:04:06:07   2103
2 red-vlan  192.168.1.5 00:01:03:04:06:08   102
2 red-vlan  192.168.1.7 00:01:03:04:06:09   16789
```

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
WX1200# display dhcp-server verbose
Interface:        0 (Direct AP)
 Status:           UP
 Address Range:    10.0.0.1-10.0.0.253

 Interface:            default(1)
 Status:               UP
 Address Range:        10.10.20.2-10.10.20.254
 DHCP Clients:
   Hardware Address:     00:01:02:03:04:05
   State:                BOUND
   Lease Allocation:     43200 seconds
   Lease Remaining:      12345 seconds
   IP Address:           10.10.20.2
   Subnet Mask:          255.255.255.0
```

Downloaded from www.Manualslib.com manuals search engine

```
Default Gateway:      10.10.20.1
DNS Servers:          10.10.20.4 10.10.20.5
DNS Domain Name:      mycorp.com
```

Table 31 and Table 32 describe the fields in these displays.

Table 31 Output for display dhcp-server

Field	Description
VLAN	VLAN number
Name	VLAN name
Address	IP address leased by the server.
MAC Address	MAC address of the device that holds the least for the address.
Lease Remaining	Number of seconds remaining before the address lease expires.

Table 32 Output for display dhcp-server verbose

Field	Description
Interface	VLAN name and number.
Status	Status of the interface: ■ UP ■ DOWN
Address Range	Range from which the server can lease addresses.
Hardware Address	MAC address of the DHCP client.
Lease Remaining	Number of seconds remaining before the address lease expires.
State	State of the address lease: ■ SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected. ■ CHECKING—MSS is using ARP to verify whether the address is available. ■ OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address. ■ BOUND—The client accepted the address. ■ HOLDING—The address is already in use and is therefore unavailable.
Lease Allocation	Duration of the address lease, in seconds.
Lease Remaining	Number of seconds remaining before the address lease expires.

Downloaded from www.Manualslib.com manuals search engine

Table 32 Output for display dhcp-server verbose

Field	Description
IP Address	IP address leased to the client.
Subnet Mask	Network mask of the IP address leased to the client.
Default Gateway	Default gateway IP address included in the DHCP Offer to the client.
DNS Server	DNS server IP address(es) included in the DHCP Offer to the client.
DNS Domain Name	Default DNS domain name included in the DHCP Offer to the client.

See Also

- **set interface dhcp-server** on page 162

display interface

Shows the IP interfaces configured on the wireless LAN switch.

Syntax — **`display interface`** [*`vlan-id`*]

- *`vlan-id`* — VLAN name or number.

Defaults — If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

Usage — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays all the IP interfaces configured on a WX switch:

```
WX4400# display interface
VLAN Name            Address         Mask            Enabled State   RIB
---- --------------- --------------- --------------- ------- ----- -------
   1 default         10.10.10.10     255.255.255.0   YES     Up    ipv4
   2 mauve           10.10.20.10     255.255.255.0   NO      Down  ipv4
4094 web-aaa         10.10.10.1      255.255.255.0   YES     Up    ipv4
```

Table 33 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 33 Output for display interface

Field	Description
VLAN	VLAN number
Name	VLAN name
Address	IP address
Mask	Subnet mask
Enabled	Administrative state: ▪ YES (enabled) ▪ NO (disabled)
State	Link state: ▪ Up (operational) ▪ Down (unavailable)
RIB	Routing Information Base

See Also

- **clear interface** on page 127
- **set interface** on page 160
- **set interface dhcp-client** on page 161

display ip alias

Shows the IP aliases configured on the wireless LAN switch.

Syntax — **`display ip alias`** [*`name`*]

- *`name`* — Alias string.

Defaults — If you do not specify an alias name, all aliases are displayed.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays all the aliases configured on a WX switch:

```
WX4400# display ip alias
Name                    IP Address
--------------------    --------------------
HR1                     192.168.1.2
payroll                 192.168.1.3
radius1                 192.168.7.2
```

Downloaded from www.Manualslib.com manuals search engine

Table 34 describes the fields in this display.

Table 34 Output for display ip alias

Field	Description
Name	Alias string.
IP Address	IP address associated with the alias.

See Also

- **clear ip alias** on page 128
- **set ip alias** on page 164

display ip dns

Shows the DNS servers the wireless LAN switch is configured to use.

Syntax — **`display ip dns`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays the DNS information:

```
WX4400# display ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                Type
-----------------------------------
10.1.1.1                  PRIMARY
10.1.1.2                  SECONDARY
10.1.2.1                  SECONDARY
```

Table 35 describes the fields in this display.

Table 35 Output for display ip dns

Field	Description
Domain Name	Default domain name configured on the WX switch

Downloaded from www.Manualslib.com manuals search engine

Table 35 Output for display ip dns (continued)

Field	Description
DNS Status	Status of the WX switch's DNS client: ▪ Enabled ▪ Disabled
IP Address	IP address of the DNS server
Type	Server type: ▪ PRIMARY ▪ SECONDARY

See Also

- **clear ip dns domain** on page 129
- **clear ip dns server** on page 129
- **set ip dns** on page 164
- **set ip dns domain** on page 165
- **set ip dns server** on page 166

display ip https

Shows information about the HTTPS management port.

Syntax — **`display ip https`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command shows the status and port number for the HTTPS management interface to the WX switch:

```
WX4400# display ip https
HTTPS is enabled
HTTPS is set to use port 443

Last 10 Connections:
 IP Address     Last Connected          Time Ago (s)
------------    ---------------------- ------------
10.10.10.56     2003/05/09 15:51:26 pst          349
```

Table 36 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 36 Output for display ip https

Field	Description
HTTPS is enabled/disabled	State of the HTTPS server: ■ Enabled ■ Disabled
HTTPS is set to use port	TCP port number on which the WX switch listens for HTTPS connections.
Last 10 connections	List of the last 10 devices to establish connections to the WX switch's HTTPS server.
IP Address	IP address of the device that established the connection. If a browser connects to a WX switch from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.
Last Connected	Time when the WX switch established the HTTPS connection to the WX switch.
Time Ago (s)	Number of seconds since the device established the HTTPS connection to the WX switch.

See Also

- **clear ip telnet** on page 131
- **display ip telnet** on page 148
- **set ip https server** on page 167
- **set ip telnet** on page 171
- **set ip telnet server** on page 172

display ip route

Shows the IP route table.

Syntax — **`display ip route`** [*`destination`*]

- *`destination`* — Route destination IP address, in dotted decimal notation.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — When you add an IP interface to a VLAN that is up, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the **display vlan config** command to check the VLAN state.

If you add a static route and the route's state is shown as Down, use the **display interface** command to verify that the route has an IP interface in the gateway router's subnet. MSS cannot resolve a static route unless one of the WX switch's VLANs has an interface in the gateway router's subnet. If the WX switch has such an interface but the static route is still down, use the **display vlan config** command to check the state of the VLAN's ports.

Examples — The following command shows all routes in a WX switch's IP route table:

```
WX4400# display ip route
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway         VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       Down
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
      10.0.2.1/24 IP            0 Direct                  vlan:2:ip
      10.0.2.1/32 IP            0 Direct                  vlan:2:ip:10.0.1.1/24
    10.0.2.255/32 IP            0 Direct                  vlan:2:ip:10.0.1.1/24
     224.0.0.0/ 4 IP            0 Local                   MULTICAST
```

Table 37 describes the fields in this display.

Table 37 Output of display ip route

Field	Description
Destination/Mask	IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by MSS and supports the IGMP snooping feature.
Proto	Protocol that added the route to the IP route table. The protocol can be one of the following: ▪ **IP** — MSS added the route. ▪ **Static** — An administrator added the route.
Metric	Cost for using the route.

Downloaded from www.Manualslib.com manuals search engine

Table 37 Output of display ip route (continued)

Field	Description
NH-Type	Next-hop type: ▪ **Local** — Route is for a local interface. MSS adds the route when you configure an IP address on the WX switch. ▪ **Direct** — Route is for a locally attached subnet. MSS adds the route when you add an interface in the same subnet to the WX switch. ▪ **Router** — Route is for a remote destination. A WX switch forwards traffic for the destination to the gateway router.
Gateway	Next-hop router for reaching the route destination. This field applies only to static routes.
VLAN:Interface	Destination VLAN, protocol type, and IP address of the route. Because direct routes are for local interfaces, a destination IP address is not listed. The destination for the IP multicast route is MULTICAST. For static routes, the value Down means the WX switch does not have an interface to the destination's next-hop router. To provide an interface, configure an IP interface that is in the same IP subnet as the next-hop router. The IP interface must be on a VLAN containing the port that is attached to the gateway router.

See Also

- **clear ip route** on page 130
- **display interface** on page 142
- **display vlan config** on page 111
- **set interface** on page 160
- **set ip route** on page 167

display ip telnet

Shows information about the Telnet management port.

Syntax — **`display ip telnet`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows the status and port number for the Telnet management interface to the WX switch:

```
WX4400> display ip telnet

Server Status                 Port
---------------------------------
Enabled                        23
```

Table 38 describes the fields in this display.

Table 38 Output for display ip telnet

Field	Description
Server Status	State of the HTTPS server: ▪ Enabled ▪ Disabled
Port	TCP port number on which the WX switch listens for Telnet management traffic.

See Also

- **clear ip telnet** on page 131
- **display ip https** on page 145
- **set ip https server** on page 167
- **set ip telnet** on page 171
- **set ip telnet server** on page 172

display ntp

Shows NTP client information.

Syntax — **`display ntp`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — To display NTP information for a WX switch, type the following command:

```
WX4400> display ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server          Peer state          Local State
-------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
```

Table 39 describes the fields in this display.

Table 39 Output for display ntp

Field	Description
NTP client	State of the NTP client. The state can be one of the following: ▪ Enabled ▪ Disabled
Current update-interval	Number of seconds between queries sent by the WX switch to the NTP servers for updates.
Current time	System time that was current on the WX switch when you pressed Enter after typing the **display ntp** command.
Timezone	Time zone configured on the WX switch. MSS offsets the time reported by the NTP server based on the time zone. This field is displayed only if you change the time zone.
Summertime	Summertime period configured on the WX switch. MSS offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set. This field is displayed only if you enable summertime.
Last NTP update	Time when the WX switch received the most recent update from an NTP server.
NTP Server	IP address of the NTP server.

Downloaded from www.Manualslib.com manuals search engine

Table 39 Output for display ntp (continued)

Field	Description
Peer state	State of the NTP session from the point of view of the NTP server: ▪ CORRECT ▪ REJECT ▪ SELCAND ▪ SYNCCAND ▪ SYSPEER
Local state	State of the NTP session from the point of view of the WX switch's NTP client: ▪ INITED ▪ START ▪ SYNCED

See Also

- **clear ntp server** on page 131
- **clear summertime** on page 135
- **clear timezone** on page 136
- **display timezone** on page 155
- **set ntp** on page 173
- **set ntp server** on page 174
- **set summertime** on page 191
- **set timezone** on page 194

display snmp community

Displays the configured SNMP community strings.

Syntax — **`display snmp community`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear snmp community** on page 133
- **set snmp community** on page 175

---

display snmp counters

Displays SNMP statistics counters.

Syntax — **`display snmp counters`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

---

display snmp notify profile

Displays SNMP notification profiles.

Syntax — **`display snmp notify profile`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **clear snmp notify profile** on page 133
- **set snmp notify profile** on page 177

---

display snmp notify target

Displays SNMP notification targets.

Syntax — **`display snmp notify target`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear snmp notify target** on page 134
- **set snmp notify target** on page 181

---

display snmp status

Displays SNMP version and status information.

Syntax — **`display snmp status`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **set snmp community** on page 175
- **set snmp notify target** on page 181
- **set snmp notify profile** on page 177
- **set snmp protocol** on page 186
- **set snmp security** on page 187
- **set snmp usm** on page 188
- **display snmp community** on page 151
- **display snmp counters** on page 152
- **display snmp notify profile** on page 152
- **display snmp notify target** on page 152
- **display snmp usm** on page 154

Downloaded from www.Manualslib.com manuals search engine

display snmp usm

Displays information about SNMPv3 users.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **clear snmp usm** on page 134
- **display snmp usm** on page 154

display summertime

Shows a wireless LAN switch's offset from its real-time clock.

Syntax — **`display summertime`**

Defaults — There is no summertime offset by default.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — To display the summertime setting on a WX switch, type the following command:

```
WX1200# display summertime
Summertime is enabled, and set to 'PDT'.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
              and ending at 2:00 am on last Sunday of October.
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display timedate** on page 155
- **display timezone** on page 155
- **set summertime** on page 191

Downloaded from www.Manualslib.com manuals search engine

- **set timedate** on page 193
- **set timezone** on page 194

display timedate

Shows the date and time of day currently set on a wireless LAN switch's real-time clock.

Syntax — **`display timedate`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — To display the time and date set on a WX switch's real-time clock, type the following command:

```
WX1200# display timedate
Sun Feb 29 2004, 23:59:02 PST
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display summertime** on page 154
- **display timezone** on page 155
- **set summertime** on page 191
- **set timedate** on page 193
- **set timezone** on page 194

display timezone

Shows the time offset for the real-time clock from UTC on a wireless LAN switch.

Syntax — **`display timezone`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — To display the offset from UTC, type the following command:

```
WX4400# display timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display summertime** on page 154
- **display timedate** on page 155
- **set summertime** on page 191
- **set timedate** on page 193
- **set timezone** on page 194

ping

Tests IP connectivity between a wireless LAN switch and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified WX switch and listens for a reply packet.

Syntax — **ping** *host* [**count** *num-packets*] [**dnf**] [**flood**] [**interval** *time*] [**size** *size*] [**source-ip** *ip-addr* | *vlan-name*]

- *host* — IP address, MAC address, hostname, alias, or user to ping.
- **count** *num-packets* — Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command.
- **dnf** — Enables the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
- **flood** — Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater.

Use the flood option sparingly. This option creates a lot of traffic and can affect other traffic on the network.

- **interval** *time* — Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
- **size** *size* — Packet size, in bytes. You can specify from 56 through 65,507.

Downloaded from www.Manualslib.com manuals search engine

Because the WX switch adds header information, the ICMP packet size is 8 bytes larger than the size you specify.

- **source-ip** *ip-addr* — IP address, in dotted decimal notation, to use as the source IP address in the ping packets.
- **source-ip** *vlan-name* — VLAN name to use as the ping source. MSS uses the IP address configured on the VLAN as the source IP address in the ping packets.

Defaults

- **count** — 5.
- **dnf** — Disabled.
- **interval** — 100 (one tenth of a second)
- **size** — 56.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To stop a ping command that is in progress, press Ctrl+C.

Examples — The following command pings a WX switch that has IP address 10.1.1.1:

```
WX1200# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

See Also

- **traceroute** on page 197

Downloaded from www.Manualslib.com manuals search engine

set arp

Adds an ARP entry to the ARP table.

Syntax — **set arp** {**permanent** | **static** | **dynamic** } *ip-addr mac-addr*

- **permanent** — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
- **dynamic** — Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
- *ip-addr* — IP address of the entry, in dotted decimal notation.
- *mac-addr* — MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

Defaults — The default aging timeout is 1200 seconds.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
WX1200# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

See Also

- **set arp agingtime** on page 159
- **telnet** on page 195

Downloaded from www.Manualslib.com manuals search engine

set arp agingtime

Changes the aging timeout for dynamic ARP entries.

Syntax — **`set arp agingtime`** *`seconds`*

- *`seconds`* — Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

Defaults — None.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Usage — Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Examples — The following command changes the ARP aging timeout to 1800 seconds:

```
WX1200# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
WX1200# set arp agingtime 0
success: set arp aging time to 0 seconds
```

See Also

- **set arp** on page 158
- **telnet** on page 195

Downloaded from www.Manualslib.com manuals search engine

set interface

Configures an IP interface on a VLAN.

Syntax — **`set interface`** *`vlan-id`* **`ip`** {*`ip-addr mask`* | *`ip-addr/mask-length`*}

- *`vlan-id`* — VLAN name or number.
- *`ip-addr mask`* — IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *`ip-addr/mask-length`* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

Defaults — None.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Usage — You can assign one IP interface to each VLAN.

If an interface is already configured on the VLAN you specify, this command replaces the interface. If you replace an interface that is in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — The following command configures IP interface 10.10.10.10/24 on VLAN default:

```
WX1200# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN mauve:

```
WX1200# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear interface** on page 127
- **display interface** on page 142
- **set interface dhcp-client** on page 161

set interface dhcp-client

Configures the DHCP client on a VLAN, to allow the VLAN to obtain its IP interface from a DHCP server.

Syntax — **`set interface vlan-id ip dhcp-client {enable | disable}`**

- vlan-id — VLAN name or number.
- enable — Enables the DHCP client on the VLAN.
- disable — Disables the DHCP client on the VLAN.

Defaults — The DHCP client is enabled by default on an unconfigured WXR100 when the factory reset switch is pressed and held during power on.

The DHCP client is disabled by default on all other switch models, and is disabled on a WXR100 if the switch is already configured or the factory reset switch is not pressed and held during power on.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. (See **set interface dhcp-server** on page 162.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

Examples — The following command enables the DHCP client on VLAN *corpvlan*:

```
WX1200# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear interface** on page 127
- **display dhcp-client** on page 138
- **display interface** on page 142

set interface dhcp-server

Configures the MSS DHCP server.

Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. 3Com recommends that you do not use the MSS DHCP server to allocate client addresses in a production network.

Syntax — **`set interface`** *`vlan-id`* **`ip dhcp-server [enable | disable] [start`** *`ip-addr1`* **`stop`** *`ip-addr2`***`]`**

- *`vlan-id`* — VLAN name or number.
- **`enable`** — Enables the DHCP server.
- **`disable`** — Disables the DHCP server.
- **`start`** *`ip-addr1`* — Specifies the beginning address of the address range (also called the address *pool*).
- **`stop`** *`ip-addr2`* — Specifies the ending address of the address range.

Defaults — The DHCP server is enabled by default on a new (unconfigured) WXR100, in order to provide an IP address to the host connected to the switch for access to the Web Quick Start. On all switch models, the DHCP server is enabled and cannot be disabled for directly connected MAPs.

The DHCP server is disabled by default for any other use.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
WX1200# set interface red-vlan ip dhcp-server enable start
192.168.1.5 stop 192.168.1.25
success: change accepted.
```

See Also

- **display dhcp-server** on page 140

set interface status

Administratively disables or reenables an IP interface.

Syntax — **set interface** *vlan-id* **status** {**up** | **down**}

- *vlan-id* — VLAN name or number.
- **up** — Enables the interface.
- **down** — Disables the interface.

Defaults — IP interfaces are enabled by default.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command disables the IP interface on VLAN mauve:

```
WX4400# set interface mauve status down
success: set interface mauve to down
```

See Also

- **clear interface** on page 127
- **display interface** on page 142
- **set interface** on page 160

Downloaded from www.Manualslib.com manuals search engine

set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

Syntax — **`set ip alias`** *`name ip-addr`*

- *`name`* — String of up to 32 alphanumeric characters, with no spaces.
- *`ip-addr`* — IP address in dotted decimal notation.

Defaults — None.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command configures the alias HR1 for IP address 192.168.1.2:

```
WX4400# set ip alias HR1 192.168.1.2
success: change accepted.
```

See Also

- **clear ip alias** on page 128
- **display ip alias** on page 143

set ip dns

Enables or disables DNS on a wireless LAN switch.

Syntax — **`set ip dns`** {**`enable`** | **`disable`**}

- **`enable`** — Enables DNS.
- **`disable`** — Disables DNS.

Defaults — DNS is disabled by default.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command enables DNS on a WX switch:

```
WX1200# set ip dns enable
Start DNS Client
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear ip dns domain** on page 129
- **clear ip dns server** on page 129
- **display ip dns** on page 144
- **set ip dns domain** on page 165
- **set ip dns server** on page 166

set ip dns domain

Configures a default domain name for DNS queries. The wireless LAN switch appends the default domain name to domain names or hostnames you enter in commands.

Syntax — **`set ip dns domain`** *`name`*

- *`name`* — Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

Defaults — None.

Access — Enabled.

Usage — To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is *example.com,* enter **`chris.`** if the fully qualified hostname is *chris* and not *chris.example.com.*

Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

Examples — The following command configures the default domain name *example.com*:

```
WX1200# set ip dns domain example.com
Domain name changed
```

See Also

- **clear ip dns domain** on page 129
- **clear ip dns server** on page 129
- **display ip dns** on page 144
- **set ip dns** on page 164
- **set ip dns server** on page 166

Downloaded from www.Manualslib.com manuals search engine

set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

Syntax — **set ip dns server** *ip-addr* {**primary** | **secondary**}

- *ip-addr* — IP address of a DNS server, in dotted decimal or CIDR notation.
- **primary** — Makes the server the primary server, which MSS always consults first for resolving DNS queries.
- **secondary** — Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.

Defaults — None.

Access — Enabled.

Usage — You can configure a WX switch to use one primary DNS server and up to five secondary DNS servers.

Examples — The following commands configure a WX switch to use a primary DNS server and two secondary DNS servers:

```
WX1200# set ip dns server 10.10.10.50/24 primary
success: change accepted.
WX1200# set ip dns server 10.10.20.69/24 secondary
success: change accepted.
WX1200# set ip dns server 10.10.30.69/24 secondary
success: change accepted.
```

See Also

- **clear ip dns domain** on page 129
- **clear ip dns server** on page 129
- **display ip dns** on page 144
- **set ip dns** on page 164
- **set ip dns domain** on page 165

Downloaded from www.Manualslib.com manuals search engine

set ip https server

Enables the HTTPS server on a wireless LAN switch. The HTTPS server is required for Web Manager access to the switch.

CAUTION: *If you disable the HTTPS server, Web Manager access to the WX switch is also disabled.*

Syntax — **`set ip https server`** {**`enable`** | **`disable`**}

- **`enable`** — Enables the HTTPS server.
- **`disable`** — Disables the HTTPS server.

Defaults — The HTTPS server is disabled by default.

Access — Enabled.

History — The default is changed to disabled in 3.1. In addition, the HTTPS server is no longer required for WebAAA.

Examples — The following command enables the HTTPS server on a WX switch:

```
WX1200# set ip https server enable
success: change accepted.
```

See Also

- **clear ip telnet** on page 131
- **display ip https** on page 145
- **display ip telnet** on page 148
- **set ip telnet** on page 171
- **set ip telnet server** on page 172

set ip route

Adds a static route to the IP route table.

Syntax — **`set ip route`** {**`default`** | *`ip-addr mask`* | *`ip-addr/mask-length`*} *`gateway metric`*

- **`default`** — Default route. A WX switch uses the default route if an explicit route is not available for the destination.

Default *is an alias for IP address 0.0.0.0/0.*

Downloaded from www.Manualslib.com manuals search engine

- *ip-addr mask* — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *ip-addr/mask-length* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
- *gateway* — IP address, DNS hostname, or alias of the next-hop router.
- *metric* — Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes.

Defaults — The HTTPS server is enabled by default.

Access — Enabled.

Usage — MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the **display interface** command to verify that the WX switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the **display ip route** command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique gateway address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.

When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command adds a default route that uses gateway 10.5.4.1 and gives the route a cost of 1:

```
WX4400# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the interface to that gateway router is up:

```
WX4400# set ip route default 10.2.4.69 1
success: change accepted.
WX4400# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a WX switch to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
WX4400# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
WX4400# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

See Also

- **clear ip route** on page 130
- **display interface** on page 142
- **display ip route** on page 146

set ip snmp server

Enables or disables the SNMP service on the wireless LAN switch.

Syntax — **set ip snmp server** {**enable** | **disable**}

enable — Enables the SNMP service.

disable — Disables the SNMP service.

Defaults — The SNMP service is disabled by default.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History — Introduced in MSS Version 3.0.

Examples — The following command enables the SNMP server on a WX switch:

```
WX4400# set ip snmp server enable
success: change accepted.
```

See Also

- **set port trap** on page 90
- **set snmp community** on page 175

set ip ssh

Changes the TCP port number on which a wireless LAN switch listens for Secure Shell (SSH) management traffic.

CAUTION: *If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.*

Syntax — **set ip ssh port** *port-num*

- *port-num* — TCP port number.

Defaults — The default SSH port number is 22.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the SSH port number on a WX switch to 6000:

```
WX4400# set ip ssh port 6000
success: change accepted.
```

See Also

- **set ip ssh server** on page 171

Downloaded from www.Manualslib.com manuals search engine

set ip ssh server

Disables or reenables the SSH server on a wireless LAN switch.

CAUTION: *If you disable the SSH server, SSH access to the WX switch is also disabled.*

Syntax — **`set ip ssh server`** {**`enable`** | **`disable`**}

- **`enable`** — Enables the SSH server.
- **`disable`** — Disables the SSH server.

Defaults — The SSH server is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must generate an SSH authentication key to use SSH.

The maximum number of SSH sessions supported on a WX switch is eight. If Telnet is also enabled, the WX switch can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

See Also

- **crypto generate key** on page 473
- **set ip ssh** on page 170
- **set ip ssh server** on page 171

set ip telnet

Changes the TCP port number on which a wireless LAN switch listens for Telnet management traffic.

CAUTION: *f you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the WX switch with the new Telnet port number.*

Syntax — **`set ip telnet`** *`port-num`*

- *`port-num`* — TCP port number.

Defaults — The default Telnet port number is 23.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

Examples — The following command changes the Telnet port number on a WX switch to 5000:

```
WX4400# set ip telnet 5000
success: change accepted.
```

See Also

- **clear ip telnet** on page 131
- **display ip https** on page 145
- **display ip telnet** on page 148
- **set ip https server** on page 167
- **set ip telnet server** on page 172

set ip telnet server

Enables the Telnet server on a wireless LAN switch.

CAUTION: *If you disable the Telnet server, Telnet access to the WX switch is also disabled.*

Syntax — **`set ip telnet server`** {**`enable`** | **`disable`**}

- **`enable`** — Enables the Telnet server.
- **`disable`** — Disables the Telnet server.

Defaults — The Telnet server is disabled by default.

Access — Enabled.

Usage — The maximum number of Telnet sessions supported on a WX switch is eight. If SSH is also enabled, the WX switch can have up to eight Telnet or SSH sessions, in any combination, and one console session.

Examples — The following command enables the Telnet server on a WX switch:

```
WX4400# set ip telnet server enable
success: change accepted.
```

See Also

- **clear ip telnet** on page 131

Downloaded from www.Manualslib.com manuals search engine

- **display ip https** on page 145
- **display ip telnet** on page 148
- **set ip https server** on page 167
- **set ip telnet** on page 171

set ntp

Enables or disables the NTP client on a wireless LAN switch.

Syntax — **`set ntp`** {**`enable`** | **`disable`**}

- **`enable`** — Enables the NTP client.
- **`disable`** — Disables the NTP client.

Defaults — The NTP client is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the WX time can take many NTP update intervals. 3Com recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Examples — The following command enables the NTP client:

```
WX4400# set ntp enable
success: NTP Client enabled
```

See Also

- **clear ntp server** on page 131
- **clear ntp update-interval** on page 132
- **display ntp** on page 149
- **set ntp server** on page 174
- **set ntp update-interval** on page 175

Downloaded from www.Manualslib.com manuals search engine

set ntp server

Configures a wireless LAN switch to use an NTP server.

Syntax — **`set ntp server`** *`ip-addr`*

- *`ip-addr`* — IP address of the NTP server, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.

To use NTP, you also must enable the NTP client with the **set ntp** command.

Examples — The following command configures a WX switch to use NTP server 192.168.1.5:

```
WX4400# set ntp server 192.168.1.5
```

See Also

- **clear ntp server** on page 131
- **clear ntp update-interval** on page 132
- **display ntp** on page 149
- **set ntp** on page 173
- **set ntp update-interval** on page 175

Downloaded from www.Manualslib.com manuals search engine

set ntp update-interval

Changes how often MSS sends queries to the NTP servers for updates.

Syntax — **`set ntp update-interval`** *`seconds`*

- *`seconds`* — Number of seconds between queries. You can specify from 16 through 1,024 seconds.

Defaults — The default NTP update interval is 64 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the NTP update interval to 128 seconds:

```
WX4400# set ntp update-interval 128
success: change accepted.
```

See Also

- **clear ntp server** on page 131
- **clear ntp update-interval** on page 132
- **display ntp** on page 149
- **set ntp** on page 173
- **set ntp server** on page 174

set snmp community

Configures a community string for SNMPv1 or SNMPv2c.

*For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.*

Syntax — **`set snmp community`** *`comm-string`* **`access`** {**`read-only`** | **`read-notify`** | **`notify-only`** | **`read-write`** | **`notify-read-write`**}

- *`comm-string`* — Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces.
- **`read-only`** — Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them.

Downloaded from www.Manualslib.com manuals search engine

- **read-notify** — Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications.
- **notify-only** — Allows the switch to use the string to send notifications.
- **read-write** — Allows an SNMP management application using the string to get and set object values on the switch.
- **notify-read-write** — Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Default community strings changed from *public* (for read-only) and *private* (for read-write) to blank in MSS Version 3.1. Default strings removed and new access types added for SNMPv3 (read-notify, notify-only, notify-read-write) in MSS Version 4.0.

Usage — SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. 3Com recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings *public* and *private*.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

Examples — The following command configures the read-write community *good_community*:

```
WX4400# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string *switchmgr1* with access level notify-read-write:

```
WX4400# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

See Also

- **clear snmp community** on page 133

Downloaded from www.Manualslib.com manuals search engine

- **set ip snmp server** on page 169
- **set snmp notify target** on page 181
- **set snmp notify profile** on page 177
- **set snmp protocol** on page 186
- **set snmp security** on page 187
- **set snmp usm** on page 188
- **display snmp community** on page 151

set snmp notify profile

Configures an SNMP notification profile. A *notification profile* is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

Syntax — **`set snmp notify profile`** {**`default`** | *`profile-name`*} {**`drop`** | **`send`**} {*`notification-type`* | **`all`**}

- **`default`** | *`profile-name`* — Name of the notification profile you are creating or modifying. The profile-name can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify **default**.
- **`drop | send`** — Specifies the action that the SNMP engine takes with regard to the notifications you specify with notification-type or all.
- **`notification-type`** — Name of the notification type:
  - **APBootTraps—**Generated when a MAP access point boots.
  - **ApNonOperStatusTraps**—Generated to indicate a MAP radio is nonoperational.
  - **ApOperRadioStatusTraps**—Generated when the status of a MAP radio changes.
  - **APTimeoutTraps—**Generated when a MAP access point fails to respond to the WX switch.
  - **AuthenTraps—**Generated when the WX switch's SNMP engine receives a bad community string.
  - **AutoTuneRadioChannelChangeTraps—**Generated when the RF Auto-Tuning feature changes the channel on a radio.

Downloaded from www.Manualslib.com manuals search engine

- **AutoTuneRadioPowerChangeTraps—**Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps—**Generated when a client's attempt to associate with a radio fails.
- **ClientAuthorizationSuccessTraps—**Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps—**Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps—**Generated when authorization fails for a client.
- **ClientClearedTraps—**Generated when a client's session is cleared.
- **ClientDeAssociationTraps—**Generated when a client is dissociated from a radio.
- **ClientDot1xFailureTraps—**Generated when a client experiences an 802.1X failure.
- **ClientRoamingTraps—**Generated when a client roams.
- **CounterMeasureStartTraps—**Generated when MSS begins countermeasures against a rogue access point.
- **CounterMeasureStopTraps—**Generated when MSS stops countermeasures against a rogue access point.
- **DAPConnectWarningTraps**—Generated when a Distributed MAP whose fingerprint has not been configured in MSS establishes a management session with the switch.
- **DeviceFailTraps—**Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps—**Generated when a device returns to its normal state.
- **LinkDownTraps—**Generated when the link is lost on a port.
- **LinkUpTraps—**Generated when the link is detected on a port.
- **MichaelMICFailureTraps—**Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.

Downloaded from www.Manualslib.com manuals search engine

- **MobilityDomainJoinTraps—**Generated when the WX switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
- **MobilityDomainTimeoutTraps—**Generated when a timeout occurs after a WX switch has unsuccessfully tried to communicate with a seed member.
- **PoEFailTraps—**Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user.
- **RFDetectRogueAPTraps**—Generated when MSS detects a rogue access point.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a MAP, but without the spoofed MAP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnAuthorizedAPTraps**—Generated when MSS detects the MAC address of a MAP that is on the attack list.
- **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.

Downloaded from www.Manualslib.com manuals search engine

  - **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.
- **all** — Sends or drops all notifications.

Defaults — A default notification profile (named *default*) is already configured in MSS. All notifications in the default profile are dropped by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
WX1200# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to **send** for all RF detection notification types:

```
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectDoSTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueDisappearTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueDisappearTraps
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

```
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedMacAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedSsidAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedOuiTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedSsidTraps
success: change accepted.
```

See Also

- **clear snmp notify profile** on page 133
- **set ip snmp server** on page 169
- **set snmp community** on page 175
- **set snmp notify target** on page 181
- **set snmp protocol** on page 186
- **set snmp security** on page 187
- **set snmp usm** on page 188
- **set snmp notify profile** on page 177

set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device to which MSS sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

Downloaded from www.Manualslib.com manuals search engine

Syntax — **set snmp notify target** *target-num*
ip-addr[:*udp-port-number*]
usm inform user *username*
snmp-engine-id {ip | hex *hex-string*}
[profile *profile-name*]
[security {unsecured | authenticated | encrypted}]
[retries *num*]
[timeout *num*]

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr*[:*udp-port-number*] — IP address of the server. You also can specify the UDP port number to send notifications to.
- *username* — USM username. This option is applicable only when the SNMP version is **usm**. If the user will send informs rather than traps, you also must specify the **snmp-engine-id** of the target.
- snmp-engine-id — **{ip | hex *hex-string*}** SNMP engine ID of the target. Specify ip if the target's SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use hex hex-string to specify the value.
- **profile** *profile-name* — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **security** — **{unsecured | authenticated | encrypted}** Specifies the security level, and is applicable only when the SNMP version is **usm**:
  - unsecured — Message exchanges are not authenticated, nor are they encrypted. This is the default.
  - authenticated — Message exchanges are authenticated, but are not encrypted.
  - encrypted — Message exchanges are authenticated and encrypted.
- **retries** *num* — Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
- **timeout** *num* — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

Downloaded from www.Manualslib.com manuals search engine

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

Syntax — **set snmp notify target** *target-num ip-addr*[*:udp-port-number*]
usm trap user *username*
[**profile** *profile-name*]
[**security {unsecured | authenticated | encrypted}**]

- ***target-num*** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- ***ip-addr***[***:udp-port-number***] — IP address of the server. You also can specify the UDP port number to send notifications to.
- ***username*** — USM username. This option is applicable only when the SNMP version is **usm**.
- **profile *profile-name*** — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **security — {unsecured | authenticated | encrypted}** — Specifies the security level, and is applicable only when the SNMP version is **usm**:
  - unsecured — Message exchanges are not authenticated, nor are they encrypted. This is the default.
  - authenticated — Message exchanges are authenticated, but are not encrypted.
  - encrypted — Message exchanges are authenticated and encrypted.

SNMPv2c with Informs

To configure a notification target for informs from SNMPv2c, use the following command:

Syntax — **set snmp notify target** *target-num ip-addr*[*:udp-port-number*]
v2c *community-string* **inform**
[**profile** *profile-name*]
[**retries** *num*]
[**timeout** num]

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.

Downloaded from www.Manualslib.com manuals search engine

- *ip-addr*[:*udp-port-number*] — IP address of the server. You also can specify the UDP port number to send notifications to.
- *community-string* — Community string.
- **profile** *profile-name* — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **retries** *num* — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **timeout** *num* — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv2c with Traps

To configure a notification target for traps from SNMPv2c, use the following command:

Syntax — **set snmp notify target** *target-num ip-addr*[:*udp-port-number*] **v2c** *community-string* **trap** [**profile** *profile-name*]

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr*[:*udp-port-number*] — IP address of the server. You also can specify the UDP port number to send notifications to.
- *community-string* — Community string.
- **profile** *profile-name* — Notification profile this SNMP user will use to specify the notification types to send or drop.

SNMPv1 with Traps

To configure a notification target for traps from SNMPv1, use the following command:

Syntax — **set snmp notify target** *target-num ip-addr*[:*udp-port-number*] **v1** *community-string* [**profile** *profile-name*]

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr*[:*udp-port-number*] — IP address of the server. You also can specify the UDP port number to send notifications to.

Downloaded from www.Manualslib.com manuals search engine

- *community-string* — Community string.
- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.

Defaults — The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The **inform** or **trap** option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the WX switch. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

Examples — The following command configures a notification target for acknowledged notifications:

```
WX1200# set snmp notify target 1 10.10.40.9 usm inform user
securesnmpmgr1 snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
WX1200# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

See Also

- **clear snmp notify target** on page 134
- **set ip snmp server** on page 169
- **set snmp community** on page 175
- **set snmp notify profile** on page 177

Downloaded from www.Manualslib.com manuals search engine

- **set snmp protocol** on page 186
- **set snmp security** on page 187
- **set snmp usm** on page 188
- **display snmp notify target** on page 152

set snmp protocol

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

Syntax — **`set snmp protocol {v1 | v2c | usm | all} {enable | disable}`**

- **`v1`** — SNMPv1
- **`v2c`** — SNMPv2c
- **`usm`** — SNMPv3 (with the user security model)
- **`all`** — Enables all supported versions of SNMP.
- **`enable`** — Enables the specified SNMP version(s).
- **`disable`** — Disables the specified SNMP version(s).

Defaults — All SNMP versions are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — SNMP requires the switch's system IP address to be set. SNMP will not work without the system IP address.

You also must enable the SNMP service using the **set ip snmp server** command.

Examples — The following command enables all SNMP versions:

```
WX1200# set snmp protocol all enable
success: change accepted.
```

See Also

- **set ip snmp server** on page 169
- **set snmp community** on page 175

Downloaded from www.Manualslib.com manuals search engine

- **set snmp notify target** on page 181
- **set snmp security** on page 187
- **set snmp usm** on page 188
- **display snmp status** on page 153

set snmp security

Sets the minimum level of security MSS requires for SNMP message exchanges.

Syntax — **`set snmp security {unsecured | authenticated | encrypted | auth-req-unsec-notify}`**

- **`unsecured`** — SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
- **`authenticated`** — SNMP message exchanges are authenticated but are not encrypted.
- **`encrypted`** — SNMP message exchanges are authenticated and encrypted.
- **`auth-req-unsec-notify`**— SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Defaults — By default, MSS allows nonsecure (**unsecured**) SNMP message exchanges.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

Examples — The following command sets the minimum level of SNMP security allowed to authentication ***and*** encryption:

```
WX1200# set snmp security encrypted
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set ip snmp server** on page 169
- **set snmp community** on page 175
- **set snmp notify target** on page 181
- **set snmp notify profile** on page 177
- **set snmp protocol** on page 186
- **set snmp usm** on page 188
- **display snmp status** on page 153

set snmp usm

Creates a USM user for SNMPv3.

*This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.*

Syntax — **set snmp usm** *usm-username*
snmp-engine-id {ip *ip-addr* **| local | hex** *hex-string***}**
access {read-only | read-notify | notify-only | read-write | notify-read-write}
auth-type {none | md5 | sha} {auth-pass-phrase *string* **| auth-key** *hex-string***}**
encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase *string* **| encrypt-key** *hex-string***}**

- **usm-username** — Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.
- **snmp-engine-id {ip** *ip-addr* **| local | hex** *hex-string***} —** Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify local as the engine ID.
  - **hex** *hex-string*—ID is a hexadecimal string.
  - **ip** *ip-addr*—ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.
  - **local** — Uses the value computed from the switch's system IP address.

Downloaded from www.Manualslib.com manuals search engine

- **access {read-only | read-notify | notify-only | read-write | notify-read-write}** — Specifies the access level of the user:
  - **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them.
  - **read-notify**—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.
  - **notify-only**—The switch can use the string to send notifications.
  - **read-write**—An SNMP management application using the string can get and set object values on the switch.
  - **notify-read-write** — An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications.
- **auth-type {none | md5 | sha} {auth-pass-phrase** *string* **| auth-key** *hex-string***}** — Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:
  - **none**—No authentication is used.
  - **md5**—Message-digest algorithm 5 is used.
  - **sha**—Secure Hashing Algorithm (SHA) is used.

  If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key.
  - To specify a passphrase, use the **auth-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
  - To specify a key, use the **auth-key** *hex-string* option.
- **encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase** *string* **| encrypt-key** *hex-string***}** — Specifies the encryption type used for SNMP traffic. You can specify one of the following:
  - **none**—No encryption is used. This is the default.
  - **des**—Data Encryption Standard (DES) encryption is used.
  - **3des**—Triple DES encryption is used.
  - **aes**—Advanced Encryption Standard (AES) encryption is used.

Downloaded from www.Manualslib.com manuals search engine

If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **encrypt-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the **encrypt-key** *hex-string* option.

Defaults — No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is **read-only**, and the default authentication and encryption types are both **none**.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
WX#1200 set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
WX4400# set snmp usm securesnmpmgr1 snmp-engine-id ip
192.168.40.2 auth-type sha auth-pass-phrase myauthpword
encrypt-type 3des encrypt-pass-phrase mycryptpword
success: change accepted.
```

See Also

- **clear snmp usm** on page 134
- **set ip snmp server** on page 169
- **set snmp community** on page 175
- **set snmp notify target** on page 181
- **set snmp notify profile** on page 177
- **set snmp protocol** on page 186
- **set snmp security** on page 187
- **display snmp usm** on page 154

Downloaded from www.Manualslib.com manuals search engine

set summertime

Offsets the real-time clock of a wireless LAN switch by +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.

Syntax — **`set summertime`** *`summer-name`* [**`start`** *`week weekday month hour min`* **`end`** *`week weekday month hour min`*]

- *`summer-name`* — Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like.
- **`start`** — Start of the time change period.
- *`week`* — Week of the month to start or end the time change. Valid values are **first, second, third, fourth,** or **last.**
- *`weekday`* — Day of the week to start or end the time change. Valid values are **sun, mon, tue, wed, thu, fri,** and **sat.**
- *`month`* — Month of the year to start or end the time change. Valid values are **jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov,** and **dec.**
- *`hour`* — Hour to start or end the time change — a value between 0 and 23 on the 24-hour clock.
- *`min`* — Minute to start or end the time change — a value between 0 and 59.
- **`end`** — End of the time change period.

Defaults — If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must first set the time zone with the **set timezone** command for the offset to work properly without the **start** and **end** values.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

Downloaded from www.Manualslib.com manuals search engine

Examples — To enable summertime and set the summertime time zone to PDT (Pacific Daylight Time), type the following command:

```
WX1200# set summertime PDT
success: change accepted
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display summertime** on page 154
- **display timedate** on page 155
- **display timezone** on page 155
- **set timedate** on page 193
- **set timezone** on page 194

set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Syntax — **set system ip-address** *ip-addr*

- *ip-addr* — IP address, in dotted decimal notation. The address must be configured on one of the WX switch's VLANs.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must use an address that is configured on one of the WX switch's VLANs.

To display the system IP address, use the **display system** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands configure an IP interface on VLAN taupe and configure the interface to be the system IP address:

```
WX4400# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe
WX4400# set system ip-address 10.10.20.20
success: change accepted.
```

See Also

- **clear system ip-address** on page 136
- **display system** on page 43
- **set interface** on page 160

set timedate

Sets the time of day and date on the wireless LAN switch.

Syntax — **set timedate** {**date** *mmm dd yyyy* [**time** *hh:mm:ss*]}

- **date** *mmm dd yyyy* — System date:
  - *mmm* — month
  - *dd* — day
  - *yyyy* — year
- **time** *hh:mm:ss* — System time, in hours, minutes, and seconds.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The day of week is automatically calculated from the day you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command sets the date to March 13, 2003 and time to 11:11:12:

```
WX4400# set timedate date feb 29 2004 time 23:58:00
Time now is:              Sun Feb 29 2004, 23:58:02 PST
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display summertime** on page 154
- **display timedate** on page 155
- **display timezone** on page 155
- **set summertime** on page 191
- **set timezone** on page 194

set timezone

Sets the number of hours, and optionally the number of minutes, that the wireless LAN switch's real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

Syntax — **set timezone** *zone-name* {**-***hours* [*minutes*]}

- *zone-name* — Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like.
- **-** (minus sign) — Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default.
- *hours* — Number of hours to add or subtract from UTC.
- *minutes* — Number of minutes to add or subtract from UTC.

Defaults — If this command is not used, then the default time zone is UTC.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — To set the time zone for Pacific Standard Time (PST), type the following command:

```
WX1200# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

See Also

- **clear summertime** on page 135
- **clear timezone** on page 136
- **display summertime** on page 154
- **display timedate** on page 155
- **display timezone** on page 155
- **set summertime** on page 191
- **set timedate** on page 193

telnet

Opens a Telnet client session with a remote device.

Syntax — **telnet** {*ip-addr* | *hostname*} [**port** *port-num*]

- *ip-addr* — IP address of the remote device.
- *hostname* — Hostname of the remote device.
- **port** *port-num* — TCP port number on which the TCP server on the remote device listens for Telnet connections.

Defaults — MSS attempts to establish Telnet connections with TCP port 23 by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To end a Telnet session from the remote device, press **Ctrl**+**t** or type **quit** or **logout** in the management session on the remote device. To end a client session from the local WX switch, use the **clear sessions telnet client** command.

If the configuration of the WX switch from which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the **telnet** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — In the following example, an administrator establishes a Telnet session with another device and enters a command on the remote device:

```
WX4400# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'

Copyright (c) 2004 3Com Corporation. All rights reserved.

Username: username
Password: password
WX1200-remote> display vlan
                     Admin  VLAN  Tunl                          Port
VLAN Name            Status State Affin Port              Tag   State
---- --------------- ------ ----- ----- ---------------- ----- -----
   1 default         Up     Up        5
                                        3                 none Up
   3 red             Up     Up        5
  10 backbone        Up     Up        5
                                        1                 none Up
                                        2                 none Up
4094 web-aaa         Up     Up        0
                                        2                 4094 Up
```

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local prompt:

```
WX1200-remote> Session 0 pty tty2.d terminated tt name tty2.d
WX1200#
```

See Also

- **clear sessions** on page 519
- **display sessions** on page 522

Downloaded from www.Manualslib.com manuals search engine

traceroute

Traces the route to an IP host.

Syntax — **`traceroute`** *`host`* [**`dnf`**] [**`no-dns`**] [**`port`** *`port-num`*] [**`queries`** *`num`*] [**`size`** *`size`*] [**`ttl`** *`hops`*] [**`wait`** *`ms`*]

- *`host`* — IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation.
- **`dnf`** — Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
- **`no-dns`** — Prevents MSS from performing a DNS lookup for each hop to the destination host.
- **`port`** *`port-num`* — TCP port number listening for the traceroute probes.
- **`queries`** *`num`* — Number of probes per hop.
- **`size`** *`size`* — Probe packet size in bytes. You can specify from 40 through 1,460.
- **`ttl`** *`hops`* — Maximum number of hops, which can be from 1 through 255.
- **`wait`** *`ms`* — Probe wait in milliseconds. You can specify from 1 through 100,000.

Defaults

- **dnf** — Disabled
- **no-dns** — Disabled
- **port** — 33434
- **queries** — 3
- **size** — 38
- **ttl** — 30
- **wait** — 5000

Access — All.

History —Introduced in MSS Version 3.0.

Usage — To stop a traceroute command that is in progress, press **`Ctrl+C`**.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example traces the route to host server1:

```
WX4400# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```

The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order in which the hops occur, beginning with the hop closest to the WX switch.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the ICMP Time Exceeded message to return to the host.

An exclamation point (!) following any of these values indicates that the Port Unreachable message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before MSS received a Time Exceeded message for the packet.

If Traceroute receives an ICMP error message other than a Time Exceeded or Port Unreachable message, MSS displays one of the error codes described in Table 40 instead of displaying the round-trip time or an asterisk (*).

Table 40 describes the traceroute error messages.

Table 40 Error messages for traceroute

Field	Description
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.

Downloaded from www.Manualslib.com manuals search engine

Table 40 Error messages for traceroute (continued)

Field	Description
!F	Fragmentation needed but Do Not Fragment (DNF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

See Also

- **ping** on page 156

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

8 AAA COMMANDS

Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local WX database to help you control access locally.

(Security ACLs are packet filters. For command descriptions, see Chapter 14.)

Commands by Usage

This chapter presents AAA commands alphabetically. Use Table 41 to locate commands in this chapter based on their use.

Table 41 AAA Commands by Usage

Type	Command
Authentication	**set authentication console** on page 231
	set authentication admin on page 229
	set authentication dot1x on page 233
	set authentication mac on page 239
	set authentication last-resort on page 236
	set authentication proxy on page 241
	clear authentication admin on page 204
	clear authentication console on page 205
	clear authentication dot1x on page 206
	clear authentication last-resort on page 207
	clear authentication mac on page 208
	clear authentication proxy on page 209
	clear authentication web on page 209

Downloaded from www.Manualslib.com manuals search engine

Table 41 AAA Commands by Usage (continued)

Type	Command
Local Authorization for Password Users	**set user** on page 258
	clear user on page 215
	set user attr on page 259
	clear user attr on page 216
	set usergroup on page 261
	clear usergroup on page 217
	set user group on page 260
	clear user group on page 217
	clear usergroup attr on page 218
Local Authorization for MAC Users	**set mac-user** on page 248
	clear mac-user on page 211
	set mac-user attr on page 249
	clear mac-user attr on page 212
	set mac-usergroup attr on page 254
	clear mac-usergroup attr on page 214
	clear mac-user group on page 212
	clear mac-usergroup on page 213
Web authorization	**set web-portal** on page 262
Accounting	**set accounting {admin | console}** on page 225
	set accounting {dot1x | mac | web | last-resort} on page 227
	display accounting statistics on page 222
	clear accounting on page 203
AAA information	**display aaa** on page 219
Mobility Profiles	**set mobility-profile** on page 255
	set mobility-profile mode on page 257
	display mobility-profile on page 224
	clear mobility-profile on page 215
Location Policy	**set location policy** on page 244
	display location policy on page 224
	clear location policy on page 210

Downloaded from www.Manualslib.com manuals search engine

clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

Syntax — **`clear accounting`** {**`admin`** | **`dot1x`**} {*`user-glob`*}

- **`admin`** — Users with administrative access to the WX switch through a console connection or through a Telnet or Web Manager connection.
- **`dot1x`** — Users with network access through the WX switch. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.
- *`user-glob`* — Single user or set of users with administrative access or network access.

  Specify a username, use the double-asterisk wildcard character (**`**`**) to specify all usernames, or use the single-asterisk wildcard character (**`*`**) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**`@`**) or a period (**`.`**). (For details, see "User Globs" on page 26.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes accounting services for authorized network user Nin:

```
WX4400# clear accounting dot1x Nin
success: change accepted.
```

See Also

- **set accounting {admin | console}** on page 225
- **display accounting statistics** on page 222

Downloaded from www.Manualslib.com manuals search engine

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web Manager.

Syntax — **clear authentication admin** *user-glob*

- *user-glob* — A single user or set of users.

  Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command clears authentication for administrator Jose:

```
WX4400# clear authentication admin Jose
success: change accepted.
```

See Also

- **clear authentication console** on page 205
- **clear authentication dot1x** on page 206
- **clear authentication last-resort** on page 207
- **clear authentication mac** on page 208
- **clear authentication proxy** on page 209
- **display aaa** on page 219
- **set authentication admin** on page 229

Downloaded from www.Manualslib.com manuals search engine

clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax — **`clear authentication console`** *`user-glob`*

- *`user-glob`* — A single user or set of users.

  Specify a username, use the double-asterisk wildcard character (**`**`**) to specify all usernames, or use the single-asterisk wildcard character (**`*`**) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (**`@`**) or a period (.). (For details, see "User Globs" on page 26.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

*The syntax descriptions for the **clear authentication** commands have been separated for clarity. However, the options and behavior for the **clear authentication console** command are the same as in previous releases.*

Examples — The following command clears authentication for administrator Regina:

```
WX4400# clear authentication console Regina
success: change accepted.
```

See Also

- **clear authentication admin** on page 204
- **display aaa** on page 219
- **clear authentication dot1x** on page 206
- **clear authentication last-resort** on page 207
- **clear authentication mac** on page 208
- **clear authentication proxy** on page 209
- **set authentication console** on page 231

Downloaded from www.Manualslib.com manuals search engine

clear authentication dot1x

Removes an 802.1X authentication rule.

Syntax — **clear authentication dot1x** {**ssid** *ssid-name* | **wired**} *user-glob*

- **ssid** *ssid-name* — SSID name to which this authentication rule applies.
- **wired** — Clears a rule used for access over a WX switch's wired-authentication port.
- *user-glob* — A single user or a set of users with 802.1X network access.

  Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes 802.1X authentication for network users with usernames ending in *@thiscorp.com* who try to access SSID *finance*:

```
WX4400# clear authentication dot1x ssid finance
*@thiscorp.com
```

See Also

- **clear authentication admin** on page 204
- **clear authentication console** on page 205
- **clear authentication last-resort** on page 207
- **clear authentication mac** on page 208
- **clear authentication proxy** on page 209
- **display aaa** on page 219
- **set authentication dot1x** on page 233

Downloaded from www.Manualslib.com manuals search engine

clear authentication last-resort

Removes a last-resort authentication rule.

Syntax — **`clear authentication last-resort`** {**`ssid`** *`ssid-name`* | **`wired`**}

- **`ssid`** *`ssid-name`* —SSID name to which this authentication rule applies.
- **`wired`** — Clears a rule used for access over a WX switch's wired-authentication port.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes a last-resort authentication rule for wired-authentication access:

```
WX4400# clear authentication last-resort wired
```

See Also

- **clear authentication admin** on page 204
- **clear authentication console** on page 205
- **clear authentication dot1x** on page 206
- **clear authentication mac** on page 208
- **clear authentication proxy** on page 209
- **display aaa** on page 219
- **set authentication last-resort** on page 236

Downloaded from www.Manualslib.com manuals search engine

clear authentication mac

Removes a MAC authentication rule.

Syntax — **clear authentication mac** {**ssid** *ssid-name* | **wired**} *mac-addr-glob*

- **ssid** *ssid-name* — SSID name to which this authentication rule applies.
- **wired** — Clears a rule used for access over a WX switch's wired-authentication port.
- *mac-addr-glob* — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*****) character to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes a MAC authentication rule for access to SSID *thatcorp* by MAC addresses beginning with *aa:bb:cc:*

```
WX4400# clear authentication mac ssid thatcorp aa:bb:cc:*
```

See Also

- **clear authentication admin** on page 204
- **clear authentication console** on page 205
- **clear authentication dot1x** on page 206
- **clear authentication last-resort** on page 207
- **clear authentication proxy** on page 209
- **display aaa** on page 219
- **set authentication mac** on page 239

Downloaded from www.Manualslib.com manuals search engine

clear authentication proxy

Removes a proxy rule for third-party AP users.

Syntax — **`clear authentication proxy ssid`** *`ssid-name user-glob`*

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies.
- *`user-glob`* — User-glob associated with the rule you are removing.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command removes the proxy rule for SSID *mycorp* and userglob **:

```
WX4400# clear authentication proxy ssid mycorp
```

See Also

- **set authentication proxy** on page 241
- **display aaa** on page 219

clear authentication web

Removes a WebAAA rule.

Syntax — **`clear authentication web {ssid`** *`ssid-name`* **`| wired}`** *`user-glob`*

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies.
- **`wired`** — Clears a rule used for access over a WX switch's wired-authentication port.
- *`user-glob`* — User-glob associated with the rule you are removing.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command removes WebAAA for SSID *research* and userglob *temp*@thiscorp.com*:

```
WX4400# clear authentication web ssid research
temp*@thiscorp.com
```

See Also

- **clear authentication admin** on page 204
- **clear authentication console** on page 205
- **clear authentication dot1x** on page 206
- **clear authentication last-resort** on page 207
- **clear authentication mac** on page 208
- **set authentication web** on page 242
- **display aaa** on page 219

clear location policy

Removes a rule from the location policy on a WX switch.

Syntax — **clear location policy** *rule-number*

- *rule-number* — Index number of a location policy rule to remove from the location policy.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To determine the index numbers of location policy rules, use the **display location policy** command. Removing all the ACEs from the location policy disables this function on the WX switch.

Examples — The following command removes location policy rule 4 from an WX switch's location policy:

```
WX4400# clear location policy 4
success: clause 4 is removed.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display location policy** on page 224
- **set location policy** on page 244

---

clear mac-user

Removes a user profile from the local database on the WX switch, for a user who is authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **`clear mac-user`** *`mac-addr`*

- *`mac-addr`* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Deleting a MAC user's profile from the database deletes the assignment of any attributes in the profile to the user.

Examples — The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set mac-usergroup attr** on page 254
- **set mac-user attr** on page 249

Downloaded from www.Manualslib.com manuals search engine

clear mac-user attr

Removes an authorization attribute from the user profile in the local database on the WX switch, for a user who is authenticated by a MAC address.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear mac-user** *mac-addr* **attr** *attribute-name*

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *attribute-name* — Name of an attribute used to authorize the MAC user for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 249.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set mac-user attr** on page 249

clear mac-user group

Removes a user profile from a MAC user group in the local database on the WX switch, for a user who is authenticated by a MAC address.

(To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear mac-user** *mac-addr* **group**

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (**:**). You can omit leading zeros.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Removing a MAC user from a MAC user group removes the group name from the user's profile, but does not delete the user group from the local WX database. To remove the group, use **clear mac-usergroup**.

Examples — The following command deletes the user profile for a user at MAC address 01:02:03:04:05:06 from its user group:

```
WX4400# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

See Also

- **clear mac-usergroup** on page 213
- **display aaa** on page 219
- **set mac-user** on page 248

---

clear mac-usergroup

Removes a user group from the local database on the WX switch, for a group of users who are authenticated by a MAC address.

(To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear mac-usergroup** *group-name*

- *group-name* — Name of an existing MAC user group.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To remove a user from a MAC user group, use the **clear mac-user group** command.

Examples — The following command deletes the MAC user group *eastcoasters* from the local database:

```
WX4400# clear mac-usergroup eastcoasters
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear mac-usergroup attr** on page 214
- **display aaa** on page 219
- **set mac-usergroup attr** on page 254

---

clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the WX switch, for a group of users who are authenticated by a MAC address.

(To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear mac-usergroup** *group-name* **attr** *attribute-name*

- *group-name* — Name of an existing MAC user group.
- *attribute-name* — Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 249.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To remove the group itself, use the **clear mac-usergroup** command.

Examples — The following command removes the members of the MAC user group *eastcoasters* from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
WX4400# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

See Also

- **clear mac-usergroup** on page 213
- **display aaa** on page 219
- **set mac-usergroup attr** on page 254

Downloaded from www.Manualslib.com manuals search engine

clear mobility-profile

Removes a Mobility Profile entirely.

Syntax — **`clear mobility-profile`** *`name`*

- *`name`* — Name of an existing Mobility Profile.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes the Mobility Profile for user Nin:

```
WX1200# clear mobility-profile Nin
success: change accepted.
```

See Also

- **set mobility-profile** on page 255
- **set mobility-profile mode** on page 257
- **display mobility-profile** on page 224

clear user

Removes a user profile from the local database on the WX switch, for a user with a password.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **`clear user`** *`username`*

- *`username`* — Username of a user with a password.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Deleting the user's profile from the database deletes the assignment of any attributes in the profile to the user.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command deletes the user profile for user Nin:

```
WX4400# clear user Nin
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set user** on page 258

clear user attr

Removes an authorization attribute from the user profile in the local database on the WX switch, for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax — **clear user** *username* **attr** *attribute-name*

- *username* — Username of a user with a password.
- *attribute-name* — Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 249.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes the Session-Timeout attribute from Hosni's user profile:

```
WX4400# clear user Hosni attr session-timeout
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set user attr** on page 259

Downloaded from www.Manualslib.com manuals search engine

clear user group

Removes a user with a password from membership in a user group in the local database on the WX switch.

(To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — **`clear user`** *`username`* **`group`**

- *`username`* — Username of a user with a password.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Removing the user from the group removes the group name from the user's profile, but does not delete either the user or the user group from the local WX database. To remove the group, use **clear usergroup**.

Examples — The following command removes the user Nin from a user group:

```
WX4400# clear user Nin group
success: change accepted.
```

See Also

- **clear usergroup** on page 217
- **display aaa** on page 219
- **set user group** on page 260

clear usergroup

Removes a user group and its attributes from the local database on the WX switch, for users with passwords.

(To delete a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — **`clear usergroup`** *`group-name`*

- *`group-name`* — Name of an existing user group.

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Removing a user group from the local WX database does not remove the user profiles of the group's members from the database.

Examples — The following command deletes the *cardiology* user group from the local database:

```
WX4400# clear usergroup cardiology
success: change accepted.
```

See Also

- **clear usergroup attr** on page 218
- **display aaa** on page 219
- **set usergroup** on page 261

---

clear usergroup attr

Removes an authorization attribute from a user group in the local database on the WX switch.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear usergroup** *group-name* **attr** *attribute-name*

- *group-name* — Name of an existing user group.
- *attribute-name* — Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 249.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command removes the members of the user group *cardiology* from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
WX4400# clear usergroup cardiology attr time-of-day
success: change accepted.
```

See Also

- **clear usergroup** on page 217
- **display aaa** on page 219
- **set usergroup** on page 261

display aaa

Displays all current AAA settings.

Syntax — **display aaa**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Web Portal section added, to indicate the state of the WebAAA feature in MSS Version 4.0.

Examples — To display all current AAA settings, type the following command:

```
WX4400# display aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                  Addr           Ports   T/o Tries Dead State
-------------------------------------------------------------------
rs-3                198.162.1.1     1821 1813  5    3    0    UP
rs-4                198.168.1.2     1821 1813  77   11   2    UP
rs-5                198.162.1.3     1821 1813  42   23   0    UP
Server groups
sg1: rs-3
sg2: rs-4
sg3: rs-5

Web Portal:
enabled
```

Downloaded from www.Manualslib.com manuals search engine

```
set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dot1x ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local
set authentication last-resort ssid guestssid local

user Nin
Password = 082c6c64060b (encrypted)
Filter-Id = acl-999.in
Filter-Id = acl-999.out
user last-resort-guestssid
Vlan-Name = k2
user last-resort-any
Vlan-Name = foo
mac-user 01:02:03:04:05:06
usergroup eastcoasters
   session-timeout = 99
```

Table 42 describes the fields that can appear in **display aaa** output.

Table 42 display aaa Output

Field	Description
Default Values	RADIUS default values for all parameters.
authport	UDP port on the WX switch for transmission of RADIUS authorization and authentication messages. The default port is 1812.
acctport	UDP port on the WX switch for transmission of RADIUS accounting records. The default is port 1813.
timeout	Number of seconds the WX switch waits for a RADIUS server to respond before retransmitting. The default is 5 seconds.
acct-timeout	Number of seconds the WX switch waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds.
retrans	Number of times the WX switch retransmits a message before determining a RADIUS server unresponsive. The default is 3 times.

Downloaded from www.Manualslib.com manuals search engine

Table 42 display aaa Output (continued)

deadtime	Number of minutes the WX switch waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the WX switch. The default is 0 minutes.
key	Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key.
author-pass	Password used for outbound authentication to a RADIUS server, used in conjunction with a last-resort username. By default, a MAC user's MAC address is also used as that user's password, and no global password is set.
Radius Servers	Information about active RADIUS servers.
Server	Name of each RADIUS server currently active.
Addr	IP address of each RADIUS server currently active.
Ports	UDP ports that the WX switch uses for authentication messages and for accounting records.
T/o	Setting of timeouts on each RADIUS server currently active.
Tries	Number of retransmissions configured for each RADIUS server currently active. The default is 3 times.
Dead	Length of time until the server is considered responsive again.
State	Current state of each RADIUS server currently active: ▪ UP (operating) ▪ DOWN (unavailable)
Server groups	Names of RADIUS server groups and member servers configured on the WX switch.
Web Portal	State of the WebAAA feature: ▪ enabled ▪ disabled
set commands	List of commands used to configure AAA on the WX switch.
user and user group profiles	List of user and user group profiles stored in the local database on the WX switch.

See Also

- **set accounting {admin | console}** on page 225
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication dot1x** on page 233

Downloaded from www.Manualslib.com manuals search engine

- **set authentication last-resort** on page 236
- **set authentication mac** on page 239
- **set authentication web** on page 242

display accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the WX switch.

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax — **`display accounting statistics`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To display the locally stored accounting records, type the following command:

```
WX4400# display accounting statistics
Sep 26 11:01:48 Acct-Status-Type=START Acct-Authentic=2
User-Name=geetha AAA_TTY_ATTR=2 Event-Timestamp=1064599308
Sept 26 12:50:21 Acct-Status-Type=STOP Acct-Authentic=2
User-Name=geetha AAA_TTY_ATTR=2 Acct-Session-Time=6513
Event-Timestamp=1064605821 Acct-Output-Octets=332
Acct-Input-Octets=61
Sep 26 12:50:33 Acct-Status-Type=START Acct-Authentic=2
User-Name=geetha AAA_TTY_ATTR=2 Event-Timestamp=1064605833
```

Table 43 describes the fields that can appear in **display accounting statistics** output.

Table 43 display accounting statistics Output

Field	Description
Date and time	Date and time of the accounting record.

Downloaded from www.Manualslib.com manuals search engine

Table 43 display accounting statistics Output (continued)

Acct-Status-Type	Type of accounting record: ▪ START ▪ STOP ▪ UPDATE
Acct-Authentic	Location where the user was authenticated (if authentication took place) for the session: ▪ **1** — RADIUS server ▪ **2** — Local WX database
User-Name	Username of a user with a password.
Acct-Multi-Session-Id	Unique accounting ID for multiple related sessions in a log file.
AAA_TTY_ATTR	For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number.
Event-Timestamp	Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.)
Acct-Session-Time	Number of seconds that the session has been online.
Acct-Output-Octets	Number of octets the WX switch has sent during the session.
Acct-Input-Octets	Number of octets the WX switch has received during the session.
Acct-Output-Packets	Number of packets the WX switch has sent during the session.
Acct-Input-Packets	Number of packets the WX switch has received during the session.
Vlan-Name	Name of the client's VLAN.
Calling-Station-Id	MAC address of the supplicant (client).
Nas-Port-Id	Number of the port and radio on the MAP access point through which the session was conducted.
Called-Station-Id	MAC address of the MAP access point through which the client reached the network.

See Also

- **clear accounting** on page 203
- **display aaa** on page 219
- **set accounting {admin | console}** on page 225

Downloaded from www.Manualslib.com manuals search engine

display location policy

Displays the list of location policy rules that make up the location policy on an WX switch.

Syntax — **`display location policy`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays the list of location policy rules in the location policy on an WX switch:

```
WX4400 display location policy
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```

See Also

- **clear location policy** on page 210
- **set location policy** on page 244

display mobility-profile

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the WX.

Syntax — **`display mobility-profile`** [*name*]

- *name* — Name of an existing Mobility Profile.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays the Mobility Profile *magnolia*:

```
WX1200# display mobility-profile magnolia
Mobility Profiles
Name                 Ports
=======================
magnolia          AP 2
```

See Also

- **clear mobility-profile** on page 215
- **set mobility-profile** on page 255

set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

Syntax — **set accounting** {**admin** | **console**} {*user-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

- **admin** — Users with administrative access to the WX switch through Telnet or Web Manager.
- **console** — Users with administrative access to the WX switch through a console connection.
- *user-glob* — Single user or set of users with administrative access or network access.
- Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an at sign (**@**) or a period (.). (For details, see "User Globs" on page 26.)

*This option does not apply if **mac** is specified. For **mac**, specify a mac-addr-glob. (See "MAC Address Globs" on page 27.)*

- **start-stop** — Sends accounting records at the start and end of a network session.
- **stop-only** — Sends accounting records only at the end of a network session.

Downloaded from www.Manualslib.com manuals search engine

- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

  A method can be one of the following:

  - **local** — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.
  - *server-group-name* — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults — Accounting is disabled for all users by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Examples — The following command issues start-and-stop accounting records at the local WX database for administrator Natasha, when she accesses the switch using Telnet or Web Manager:

```
WX4400# set accounting admin Natasha start-stop local
success: change accepted.
```

See Also

- **clear accounting** on page 203
- **display accounting statistics** on page 222

Downloaded from www.Manualslib.com manuals search engine

set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

Syntax — **set accounting** {**dot1x** | **mac** | **web** | **last-resort**} {**ssid** *ssid-name* | **wired**} {*user-glob* | *mac-addr-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

- **dot1x** — Users with network access through the WX switch who are authenticated by 802.1X.
- **mac** — Users with network access through the WX switch who are authenticated by MAC authentication
- **web** — Users with network access through the WX switch who are authenticated by WebAAA
- **ssid** *ssid-name* — SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type any.
- **wired** — Applies this accounting rule specifically to users who are authenticated on a wired authentication port.
- **user-glob** — Single user or set of users with administrative access or network access.

  Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character — either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)

*This option does not apply if **mac** or **last-resort** is specified. For **mac**, specify a mac-addr-glob. (See "MAC Address Globs" on page 27.)*

- *mac-addr-glob* — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)

  This option applies only when **mac** is specified.
- **start-stop** — Sends accounting records at the start and end of a network session.
- **stop-only** — Sends accounting records only at the end of a network session.

Downloaded from www.Manualslib.com manuals search engine

- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

  A method can be one of the following:

  - **local** — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.
  - *server-group-name* — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults — Accounting is disabled for all users by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Examples — The following command issues stop-only records to the RADIUS server group *sg2* for network user Nin, who is authenticated by 802.1X:

```
WX4400# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

See Also

- **clear accounting** on page 203
- **display accounting statistics** on page 222

Downloaded from www.Manualslib.com manuals search engine

set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web Manager.

Syntax — **`set authentication admin`**
`user-glob method1 [method2] [method3] [method4]`

- *`user-glob`* — Single user or set of users with administrative access over the network through Telnet or Web Manager.

  Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**@**) or a period (.). (For details, see "User Globs" on page 26.)

- *`method1, method2, method3, method4`* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **`local`** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *`server-group-name`* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
  - **`none`** — *For users with administrative access only,* MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

*The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the WX switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See "set service-profile auth-fallthru" on page 374.)*

For more information, see "Usage."

Defaults — By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**. MSS checks the local WX database for authentication.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

*The syntax descriptions for the **set authentication** commands have been separated for clarity. However, the options and behavior for the **set authentication admin** command are the same as in previous releases.*

Usage — You can configure different authentication methods for different groups of users. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 26.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and MSS authenticates a client with the local method, MSS starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Examples — The following command configures administrator Jose, who connects via Telnet, for authentication on RADIUS server group *sg3*:

```
WX4400# set authentication admin Jose sg3
success: change accepted.
```

See Also

- **clear authentication admin** on page 204
- **display aaa** on page 219
- **set authentication console** on page 231
- **set authentication dot1x** on page 233
- **set authentication last-resort** on page 236

Downloaded from www.Manualslib.com manuals search engine

- **set authentication mac** on page 239
- **set authentication web** on page 242

set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

Syntax — **`set authentication console`**
`user-glob method1 [method2] [method3] [method4]`

- *`user-glob`* — Single user or set of users with administrative access through the switch's console.

  Specify a username, use the double-asterisk wildcard character (**`**`**) to specify all usernames, or use the single-asterisk wildcard character (**`*`**) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**@**) or a period (.). (For details, see "User Globs" on page 26.)

- *`method1, method2, method3, method4`* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **`local`** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *`server-group-name`* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
  - **`none`** — *For users with administrative access only,* MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

*The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the WX switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See "set service-profile auth-fallthru" on page 374.)*

Downloaded from www.Manualslib.com manuals search engine

Defaults — By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is **none**. MSS requires no username or password, by default. These users can press Enter at the prompts for administrative access.

3Com recommends that you change the default setting unless the WX switch is in a secure physical location.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 26.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

Examples — To set the console port so that it does *not* enforce username-password authentication for administrators, type the following command:

```
WX4400# set authentication console * none
success: change accepted.
```

See Also

- **clear authentication console** on page 205
- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication dot1x** on page 233
- **set authentication last-resort** on page 236

Downloaded from www.Manualslib.com manuals search engine

- **set authentication mac** on page 239
- **set authentication web** on page 242

set authentication dot1x

Configures authentication and defines how and where it is performed for specified wireless or wired authentication clients who use an IEEE 802.1X authentication protocol to access the network through the WX switch.

Syntax — **`set authentication dot1x`** {**`ssid`** *`ssid-name`* | **`wired`**} *`user-glob`* [**`bonded`**] *`protocol method1`* [*`method2`*] [*`method3`*] [*`method4`*]

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **`wired`** — Applies this authentication rule specifically to users connected to a wired authentication port.
- *`user-glob`* — A single user or a set of users with 802.1X network access.

  Specify a username, use the double-asterisk wildcard character (**`**`**) to specify all usernames, or use the single-asterisk wildcard character (**`*`**) to specify a set of usernames up to or following the first delimiter character — either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)
- **`bonded`** — Enables Bonded Auth™ (bonded authentication). When this feature is enabled, MSS authenticates the user only if the machine the user is on has already been authenticated.
- *`protocol`* — Protocol used for authentication. Specify one of the following:
  - **`eap-md5`** — Extensible Authentication Protocol (EAP) with message-digest algorithm 5. *For wired authentication clients*:

    Uses challenge-response to compare hashes

    Provides *no* encryption or integrity checking for the connection
  - **`eap-tls`** — EAP with Transport Layer Security (TLS):

    Provides mutual authentication, integrity-protected negotiation, and key exchange

    Requires X.509 public key certificates on both sides of the connection

Downloaded from www.Manualslib.com manuals search engine

Provides encryption and integrity checking for the connection

Cannot be used with RADIUS server authentication (requires user information to be in the switch's local database)

- **peap-mschapv2** — Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). *For wireless clients*:

  Uses TLS for encryption and data integrity checking and server-side authentication

  Provides MS-CHAP-V2 mutual authentication

  Only the server side of the connection needs a certificate.

  The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method.

- **pass-through** — MSS sends all the EAP protocol processing to a RADIUS server.

EAP-MD5 does not work with Microsoft wired authentication clients.

- *method1*, *method2*, *method3*, *method4* — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

    RADIUS servers cannot be used with the EAP-TLS protocol.

  For more information, see "Usage."

Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 26.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

You cannot configure client authentication that uses both the EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local WX database.

If you specify multiple authentication methods in the **set authentication dot1x** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

If the user does not support 802.1X, MSS attempts to perform MAC authentication for the user. In this case, if the switch's configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web** (for WebAAA), or **none**.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures EAP-TLS authentication in the local WX database for SSID *mycorp* and 802.1X client Geetha:

```
WX4400# set authentication dot1x ssid mycorp Geetha eap-tls
local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups *sg1* through *sg3* for all 802.1X clients at *example.com* who want to access SSID *examplecorp*:

```
WX4400# set authentication dot1x ssid examplecorp
*@example.com peap-mschapv2 sg1 sg2 sg3
success: change accepted.
```

See Also

- **clear authentication dot1x** on page 206
- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication last-resort** on page 236
- **set authentication mac** on page 239
- **set authentication web** on page 242
- **set service-profile auth-fallthru** on page 374

set authentication last-resort

Configures an authentication rule to grant network access to a user who is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax — **set authentication last-resort** {**ssid** *ssid-name* | **wired**} *method1* [*method2*] [*method3*] [*method4*]

- **ssid** *ssid-name* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **wired** — Applies this authentication rule specifically to users connected to a wired authentication port.

Downloaded from www.Manualslib.com manuals search engine

- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

  For more information, see "Usage."

Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users. When using RADIUS for authentication, a last-resort user's default authorization password is *3Com*.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 26.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

If you specify multiple authentication methods in the **set authentication last-resort** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.

Downloaded from www.Manualslib.com manuals search engine

However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

MSS uses a last-resort authentication rule under the following conditions:

- The client is not denied access by 802.1X or does not support 802.1X.
- The client's MAC address does not match a MAC authentication rule.
- The fallthru method is **last-resort**. (For a wireless authentication rule, the fallthru method is specified by the **set service-profile auth-fallthru** command. For a wired authentication rule, the fallthru method is specified by the **auth-fall-thru** option of the **set port type wired-auth** command.)

For wireless access, MSS appends the requested SSID name to the user name *last-resort*. For example, if the requested SSID is *mycorp*, MSS attempts to authenticate the user *last-resort-mycorp*. If the RADIUS server or local database used as the authentication method has the user *last-resort-mycorp*, access is granted. Otherwise, access is denied.

If the SSID specified in the last-resort authentication rule is **any**, MSS searches for user *last-resort-any*. The *any* in the username is not a wildcard. The username must be **last-resort-any**, exactly as spelled here.

Examples — The following command configures a last-resort authentication rule in the local WX database for SSID *mycorp*:

```
WX4400# set authentication last-resort ssid mycorp local
success: change accepted.
```

See Also

- **clear authentication last-resort** on page 207
- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication dot1x** on page 233
- **set authentication mac** on page 239
- **set authentication web** on page 242

Downloaded from www.Manualslib.com manuals search engine

set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

Syntax — **`set authentication mac`**

{**`ssid`** *`ssid-name`* | **`wired`**} *`mac-addr-glob method1`* [*`method2`*] [*`method3`*] [*`method4`*]

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **`wired`** — Applies this authentication rule specifically to users connected to a wired authentication port.
- *`mac-addr-glob`* — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)
- *`method1, method2, method3, method4`* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **`local`** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *`server-group-name`* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

  For more information, see "Usage."

Defaults — By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, a MAC user's MAC address is also used as the authorization password for that user, and no global authorization password is set.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — You can configure different authentication methods for different groups of MAC addresses by "globbing." (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 26.)

If you specify multiple authentication methods in the **set authentication mac** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

If the switch's configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web** (for WebAAA), or **none**.

Examples — To use the local WX database to authenticate all users who access the *mycorp2* SSID by their MAC address, type the following command:

```
WX4400# set authentication ssid mycorp2 mac ** local
success: change accepted.
```

See Also

- **clear authentication mac** on page 208
- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication dot1x** on page 233
- **set authentication last-resort** on page 236
- **set authentication web** on page 242

Downloaded from www.Manualslib.com manuals search engine

set authentication proxy

Configures a proxy authentication rule for a third-party AP's wireless users.

Syntax — **`set authentication proxy ssid`** *`ssid-name user-glob radius-server-group`*

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies.
- *`user-glob`* — A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 26.)
- *`radius-server-group`* — A group of RADIUS servers used for authentication.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.

Examples — The following command configures a proxy authentication rule that matches on all usernames associated with SSID *mycorp*. MSS uses RADIUS server group *srvrgrp1* to proxy RADIUS requests and hence to authenticate and authorize the users.

```
WX4400# set authentication proxy ssid mycorp ** srvrgrp1
```

See Also

- **clear authentication proxy** on page 209
- **set radius proxy client** on page 492
- **set radius proxy port** on page 493

Downloaded from www.Manualslib.com manuals search engine

set authentication web

Configures an authentication rule to allow a user to log in to the network using a web page served by the WX switch. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax — `set authentication web {ssid ssid-name | wired} user-glob method1 [method2] [method3] [method4]`

- *`user-glob`* — A single user or a set of users.

  Specify a username, use the double-asterisk wildcard character (**`**`**) to specify all usernames, or use the single-asterisk wildcard character (**`*`**) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**@**) or a period (.). (For details, see "User Globs" on page 26.)

- **`ssid`** *`ssid-name`* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.

- **`wired`** — Applies this authentication rule specifically to users connected to a wired authentication port.

- *`method1`*, *`method2`*, *`method3`*, *`method4`* — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **`local`** — Uses the local database of usernames and user groups on the WX switch for authentication.
  - *`server-group-name`* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

    RADIUS servers cannot be used with the EAP-TLS protocol.

  For more information, see "Usage."

Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 26.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

If you specify multiple authentication methods in the **set authentication web** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

The client is not denied access by 802.1X or does not support 802.1X.

The client's MAC address does not match a MAC authentication rule.

The fallthru method is **web**. (For a wireless authentication rule, the fallthru method is specified by the **set service-profile auth-fallthru** command. For a wired authentication rule, the fallthru method is specified by the **auth-fall-thru** option of the **set port type wired-auth** command.)

Examples — The following command configures a WebAAA rule in the local WX database for SSID *ourcorp* and userglob *rnd**:

```
WX4400# set authentication web ssid ourcorp rnd* local
success: change accepted.
```

See Also

- **clear authentication proxy** on page 209

Downloaded from www.Manualslib.com manuals search engine

- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication dot1x** on page 233
- **set authentication last-resort** on page 236

set location policy

Creates and enables a location policy on an WX switch. The location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

Syntax — **set location policy deny if** {ssid *operator ssid-name* | **vlan** *operator vlan-glob* | **user** *operator user-glob* | **port** *port-list* | **dap** *dap-num}* [**before** *rule-number* | **modify** *rule-number*]

Syntax — **set location policy permit** {**vlan** *vlan-name* | **inacl** *inacl-name* | **outacl** *outacl-name}* **if** {**ssid** *operator ssid-name* | **vlan** *operator vlan-glob* | **user** *operator user-glob* | **port** *port-list* | **dap** *dap-num*} [**before** *rule-number* | **modify** *rule-number*]

- **deny** — Denies access to the network to users with characteristics that match the location policy rule.
- **permit** — Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with characteristics that match the location policy rule.
- **Action options** — For a permit rule, MSS changes the attributes assigned to the user to the values specified by the following options:
- **vlan** *vlan-name* — Name of an existing VLAN to assign to users with characteristics that match the location policy rule.
- **inacl** *inacl-name* — Name of an existing security ACL to apply to packets sent to the WX switch with characteristics that match the location policy rule.

  Optionally, you can add the suffix **.in** to the name.
- **outacl** *outacl-name* — Name of an existing security ACL to apply to packets sent from the WX switch with characteristics that match the location policy rule.

Downloaded from www.Manualslib.com manuals search engine

Optionally, you can add the suffix **.out** to the name.

- **`Condition options`** — MSS takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:
- **`ssid`** *`operator ssid-name`* — SSID with which the user is associated. The *operator* must be **eq**, which applies the location policy rule to all users associated with the SSID. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.
- **`vlan operator`** *`vlan-glob`* — VLAN-Name attribute assigned by AAA and condition by which to determine if the location policy rule applies. Replace operator with one of the following operands:
  - **`eq`** — Applies the location policy rule to all users assigned VLAN names matching *vlan-glob.*
  - **`neq`** — Applies the location policy rule to all users assigned VLAN names *not* matching *vlan-glob.*

  For *vlan-glob*, specify a VLAN name, use the double-asterisk wildcard character (******) to specify all VLAN names, or use the single-asterisk wildcard character (*****) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 28.)
- **`user`** *`operator user-glob`* — Username and condition by which to determine if the location policy rule applies. Replace operator with one of the following operands:
  - **`eq`** — Applies the location policy rule to all usernames matching *user-glob.*
  - **`neq`** — Applies the location policy rule to all usernames *not* matching *user-glob.*

  For *user-glob*, specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)
- **`before`** *`rule-number`* — Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the **display location policy** command.)

Downloaded from www.Manualslib.com manuals search engine

- **modify** *rule-number* — Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the **display location policy** command.)
- **port** *port-list* — List of physical port(s) by which to determine if the location policy rule applies.

Defaults — By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

Access — Enabled.

History —Introduced in MSS Version 3.0. SSID option added in MSS Version 3.2.

Usage — Only a single location policy is allowed per WX switch. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.

Conditions within a rule are ANDed. All conditions in the rule must match for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the switch's configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before** *rule-number* and **modify** *rule-number* in the **set location policy** command, and the **clear location policy** *rule-number* command.

When applying security ACLs:

Use **inacl** *inacl-name* to filter traffic that enters the switch from users via a MAP access port or wired authentication port, or from the network via a network port.

Use **outacl** *outacl-name* to filter traffic sent from the switch to users via a MAP access port or wired authentication port, or from the network via a network port.

Downloaded from www.Manualslib.com manuals search engine

You can optionally add the suffixes **.in** and **.out** to *inacl-name* and *outacl-name* so that they match the names of security ACLs stored in the local WX database.

Examples — The following command denies network access to all users at *.theirfirm.com, causing them to fail authorization:

```
WX4400# set location policy deny if user eq *.theirfirm.com
```

The following command authorizes access to the *guest_1* VLAN for all users who are not at *.wodefirm.com:

```
WX4400# set location policy permit vlan guest_1 if user neq
*.wodefirm.com
```

The following command authorizes users at *.ny.ourfirm.com to access the *bld4.tac* VLAN instead, and applies the security ACL *tac_24* to the traffic they receive:

```
WX4400# set location policy permit vlan bld4.tac
outacl tac_24 if user eq *.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names matching *bld4.** and applies security ACLs *svcs_2* to the traffic they send and *svcs_3* to the traffic they receive:

```
WX4400# set location policy permit inacl svcs_2 outacl svcs_3
if vlan eq bldg4.*
```

The following command authorizes users entering the network on WX ports 1 and 2 to use the *floor2* VLAN, overriding any settings from AAA:

```
WX4400# set location policy permit vlan floor2 if port 1-2
```

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

```
WX1200# set location policy permit vlan kiosk_1 iff ssid eq
tempvendor_a
success: change accepted
```

See Also

- **clear location policy** on page 210
- **display location policy** on page 224

Downloaded from www.Manualslib.com manuals search engine

set mac-user

Configures a user profile in the local database on the WX switch for a user who can be authenticated by a MAC address, and optionally adds the user to a MAC user group.

(To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **set mac-user** *mac-addr* [**group** *group-name*]

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *group-name* — Name of an existing MAC user group.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address can be authenticated only for network access through the WX switch. MSS does not support passwords for MAC users.

Examples — The following command creates a user profile for a user at MAC address 01:02:03:04:05:06 and assigns the user to the *eastcoasters* user group:

```
WX4400# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```

See Also

- **clear mac-user** on page 211
- **display aaa** on page 219

Downloaded from www.Manualslib.com manuals search engine

set mac-user attr

Assigns an authorization attribute in the local database on the WX switch to a user who is authenticated by a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax — **`set mac-user`** *`mac-addr`* **`attr`** *`attribute-name value`*

- *`mac-addr`* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *`attribute-name value`* — Name and value of an attribute you are using to authorize the MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 44.

Table 44 Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
encryption-type	Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.	One of the following numbers that identifies an encryption algorithm: ▪ **1**—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC) ▪ **2**—Reserved ▪ **4**—TKIP (Temporal Key Integrity Protocol) ▪ **8**—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength) ▪ **16**—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength) ▪ **32**—NONE (no encryption) ▪ **64**—Static WEP In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use **24**.

Downloaded from www.Manualslib.com manuals search engine

Table 44 Authentication Attributes for Local Users (continued)

end-date	Date and time after which the user is no longer allowed to be on the network.	Date and time, in the following format: *YY/MM/DD-HH:MM* You can use **end-date** alone or with **start-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.
filter-id	Inbound or outbound ACL to apply to the user.	If configured in the WX switch's local database, this attribute can be an access control list (ACL) to filter outbound or inbound traffic. Use the following format: **filter-id** *inboundacl***.in** or **filter-id** *outboundacl***.out** If you are configuring the attribute on a RADIUS server, the value field of filter-id can specify up to two ACLs. Any of the following are valid: filter-id = "Profile=acl1" filter-id = "OutboundACL=acl2" filter-id = "Profile=acl1 OutboundACL=acl2" (Each example goes on a single line on the server.) The format in which to specify the values depends on the RADIUS server. Regardless of whether the attributes are defined locally or on a RADIUS server, the ACLs must already be configured on the WX switch.
idle-timeout	This option is not implemented in the current MSS version.	
mobility-profile (network access mode only)	Mobility Profile attribute for the user. (For more information, see **set mobility-profile** on page 255.)	Name of an existing Mobility Profile, which can be up to 32 alphanumeric characters, with no tabs or spaces. If the Mobility Profile feature is enabled, and a user is assigned the name of a Mobility Profile that does not exist on the WX switch, the user is denied access.

Downloaded from www.Manualslib.com manuals search engine

Table 44 Authentication Attributes for Local Users (continued)

service-type	Type of access the user is requesting.	One of the following numbers: **2**—Framed; for network user access **6**—Administrative; for administrative access to the WX switch, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command to access the enabled mode. **7**—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the **enable** command is not available and the user cannot log in to the enabled mode. For administrative sessions, the WX switch will send 7 (NAS-Prompt) unless the service-type attribute has been configured for the user. The RADIUS server can reply with one of the values listed above. If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.
session-timeout (network access mode only)	Maximum number of seconds for the user's session.	Number between 0 and 4,294,967,296 seconds (approximately 136.2 years).
ssid (network access mode only)	SSID the user is allowed to access after authentication.	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to MAP radios in the Mobility Domain.
start-date	Date and time at which the user becomes eligible to access the network. MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).	Date and time, in the following format: YY/MM/DD-HH:MM You can use **start-date** alone or with **end-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.

Downloaded from www.Manualslib.com manuals search engine

Table 44 Authentication Attributes for Local Users (continued)

time-of-day
 	
(network access mode only)
	Day(s) and time(s) during which the user is permitted to log into the network.
	
	After authorization, the user's session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter.
		One of the following:
		▪ **never**—Access is always denied.
		▪ **any**—Access is always allowed.
		▪ **al**—Access is always allowed.
		▪ One or more ranges of values that consist of one of the following day designations (required), and a time range in *hhmm-hhmm* 4-digit 24-hour format (optional):
		mo—Monday
		tu—Tuesday
		we—Wednesday
		th—Thursday
		fr—Friday
		sa—Saturday
		su—Sunday
		wk—Any day between Monday and Friday
		
		Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (|). Do not use spaces.
		
		The maximum number of characters is 253.
		
		For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following:
		`time-of-day tu1000-1600,th1000-1600`
		
		To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following:
		`time-of-day wk0900-1700,sa2200-0200`
		
		(Also see the examples for **set user attr** on page 259.)
		
		You can use **time-of-day** in conjunction with **start-date**, **end-date**, or both.

Downloaded from www.Manualslib.com manuals search engine

Table 44 Authentication Attributes for Local Users (continued)

url (network access mode only)	URL to which the user is redirected after successful WebAAA.	Web URL, in standard format. For example: http://www.example.com You must include the *http://* portion. You can dynamically include any of the variables in the URL string: ▪ **$u**—Username ▪ **$v**—VLAN ▪ **$s**—SSID ▪ **$p**—Service profile name To use the literal character $ or ?, use the following: ▪ **$$** ▪ **$q**
vlan-name (network access mode only)	Virtual LAN (VLAN) assignment. On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name.	Name of a VLAN that you want the user to use. The VLAN must be configured on an WX switch within the Mobility Domain to which this WX switch belongs.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set mac-user attr** with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command assigns input access control list (ACL) *acl-03* to filter the packets from a user at MAC address 01:02:03:04:05:06:

```
WX4400# set mac-user 01:02:03:04:05:06 attr filter-id
acl-03.in
success: change accepted.
```

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
WX4400# set mac-user 06:05:04:03:02:01 attr time-of-day
mo1900-1159,tu0000-0700,we1900-1159,th0000-0700
success: change accepted.
```

See Also

- **clear mac-user attr** on page 212
- **display aaa** on page 219

---

set mac-usergroup attr

Creates a user group in the local database on the WX switch for users who are authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax — **set mac-usergroup**
group-name **attr** *attribute-name value*

- **group-name** — Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces.
- *attribute-name value* — Name and value of an attribute you are using to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 249.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — To change the value of an attribute, enter **set mac-usergroup attr** with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Examples — The following command creates the MAC user group *eastcoasters* and assigns the group members to VLAN *orange*:

```
WX4400# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

See Also

- **clear mac-usergroup attr** on page 214
- **display aaa** on page 219

set mobility-profile

Creates a Mobility Profile and specifies the MAP access point and/or wired authentication ports on the WX switch through which any user assigned to the profile is allowed access.

Syntax — **set mobility-profile name** *name* {**port** {**none** | **all** | *port-list*}} | {**dap** {**none** | **all** | *dap-num*}}

- *name* — Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.
- **none** — Prevents any user to whom this profile is assigned from accessing any MAP access point or wired authentication port on the WX switch.
- **all** — Allows any user to whom this profile is assigned to access all MAP access ports and wired authentication port on the WX switch.
- *port-list* — List of MAP access ports or wired authentication ports through which any user assigned this profile is allowed access. The same port can be used in multiple Mobility Profile port lists.

Downloaded from www.Manualslib.com manuals search engine

- *dap-num* — List of Distributed MAP connections through which any user assigned this profile is allowed access. The same Distributed MAP can be used in multiple Mobility Profile port lists.

Defaults — No default Mobility Profile exists on the WX switch. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

```
set user attr mobility-profile name
set usergroup attr mobility-profile name
set mac-user attr mobility-profile name
set mac-usergroup attr mobility-profile name
```

To enable the use of the Mobility Profile feature on the WX switch, use the **set mobility-profile mode** command.

CAUTION: *When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX switch database or RADIUS server when no Mobility Profile of that name exists on the WX switch.*

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

Examples — The following commands create the Mobility Profile *magnolia*, which restricts user access to port 2; enable the Mobility Profile feature on the WX switch; and assign the *magnolia* Mobility Profile to user *Jose*.

```
WX1200# set mobility-profile name magnolia port 2
success: change accepted.
WX1200# set mobility-profile mode enable
success: change accepted.
WX1200# set user Jose attr mobility-profile magnolia
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

The following command adds port 3 to the *magnolia* Mobility Profile (which is already assigned to port 2):

```
WX1200# set mobility-profile name magnolia port 3
success: change accepted.
```

See Also

- **clear mobility-profile** on page 215
- **display mobility-profile** on page 224
- **set mac-user attr** on page 249
- **set mac-usergroup attr** on page 254
- **set mobility-profile mode** on page 257
- **set user attr** on page 259
- **set usergroup** on page 261

set mobility-profile mode

Enables or disables the Mobility Profile feature on the WX switch.

CAUTION: *When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX switch database or RADIUS server when no Mobility Profile of that name exists on the WX switch.*

Syntax — **`set mobility-profile mode`** {**`enable`** | **`disable`**}

- **`enable`** — Enables the use of the Mobility Profile feature on the WX switch.
- **`disable`** — Specifies that all Mobility Profile attributes are ignored by the WX switch.

Defaults — The Mobility Profile feature is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To enable the use of the Mobility Profile feature, type the following command:

```
WX1200# set mobility-profile mode enable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear mobility-profile** on page 215
- **display mobility-profile** on page 224
- **set mobility-profile** on page 255

set user

Configures a user profile in the local database on the WX switch for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **`set user`** *`username`* **`password [encrypted]`** *`string`*

- *`username`* — Username of a user with a password.
- **`encrypted`** — Indicates that the password string you entered is already in its encrypted form. If you use this option, MSS does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, MSS does encrypt the displayed form of the string.
- **`password`** *`string`* — Password of up to 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Although MSS allows you to configure a user password for the special "last-resort" guest user, the password has no effect. Last-resort users can never access a WX in administrative mode and never require a password.

Examples — The following command creates a user profile for user Nin in the local database, and assigns the password *goody*:

```
WX4400# set user Nin password goody
success: User Nin created
```

Downloaded from www.Manualslib.com manuals search engine

The following command assigns the password *chey3nne* to the **admin** user:

```
WX4400# set user admin password chey3nne
success: User admin created
```

The following command changes Nin's password from *goody* to *29Jan04:*

```
WX4400# set user Nin password 29Jan04
```

See Also

- **clear user** on page 215
- **display aaa** on page 219

---

set user attr

Configures an authorization attribute in the local database on the WX switch for a user with a password.

(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax — **set user** *username* **attr** *attribute-name value*

- *username* — Username of a user with a password.
- *attribute-name value* — Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 44 on page 249.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set user attr** with the new value. To delete an attribute, use **clear user attr**.

Downloaded from www.Manualslib.com manuals search engine

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

Examples — The following command assigns user Tamara to VLAN *orange*:

```
WX4400# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command assigns Tamara to the Mobility Profile *tulip.*

```
WX4400# set user Tamara attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when user Student1 can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
WX4400# set user Student1 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

See Also

- **clear user attr** on page 216
- **display aaa** on page 219

set user group

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the WX switch.

(To configure a user in RADIUS, see the documentation for your RADIUS server.)

Syntax — **set user** *username* **group** *group-name*

- *username* — Username of a user with a password.
- *group-name* — Name of an existing user group for password users.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS does not require users to belong to user groups.

To *create* a user group, user the command **set usergroup**.

Examples — The following command adds user Hosni to the *cardiology* user group:

```
WX4400# set user Hosni group cardiology
success: change accepted.
```

See Also

- **clear user group** on page 217
- **display aaa** on page 219

---

set usergroup

Creates a user group in the local database on the WX switch for users and assigns authorization attributes for the group.

(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax — **set usergroup** *group-name* **attr** *attribute-name value*

- *group-name* — Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces.
- *attribute-name value* — Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to users, see Table 44 on page 249.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set usergroup attr** with the new value. To delete an attribute, use **clear usergroup attr**.

To *add* a user to a group, user the command **set user group**.

Downloaded from www.Manualslib.com manuals search engine

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

Examples — The following command adds the user group *cardiology* to the local database and assigns all the group members to VLAN *crimson*:

```
WX4400# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

See Also

- **clear usergroup** on page 217
- **clear usergroup attr** on page 218
- **display aaa** on page 219

set web-portal

Globally enables or disables WebAAA on a WX switch.

Syntax — **set web-portal** {**enable** | **disable**}

- **enable** — Enables WebAAA on the switch.
- **disable** — Disables WebAAA on the switch.

Defaults — Enabled.

Access — Enabled.

History —Introduced in MSS Version 3.0. Command name changed from **set web-aaa** to **set web-portal**, to match change to portal-based implementation in MSS Version 4.0.

Usage — This command disables or reenables support for WebAAA. However, WebAAA has additional configuration requirements. For information, see the "Configuring AAA for Network Users" chapter in the *Wireless LAN Switch and Controller Configuration Guide*.

Examples — To disable WebAAA, type the following command:

```
WX4400# set web-portal disable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear authentication proxy** on page 209
- **set service-profile auth-fallthru** on page 374
- **set user** on page 258

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

9 MOBILITY DOMAIN COMMANDS

Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of WX switches and MAP access points working together to support a roaming user (client). One WX switch acts as a seed switch, which maintains and distributes a list of IP addresses of the domain members.

3Com recommends that you run the same MSS version on all the WX switches in a Mobility Domain.

Commands by Usage

This chapter presents Mobility Domain commands alphabetically. Use Table 45 to locate commands in this chapter based on their use.

Table 45 Mobility Domain Commands by Usage

Type	Command
Mobility Domain	**set mobility-domain mode seed domain-name** on page 271
	set mobility-domain member on page 269
	set mobility-domain mode member seed-ip on page 270
	display mobility-domain status on page 267
	display mobility-domain config on page 267
	clear mobility-domain member on page 266
	clear mobility-domain on page 266

Downloaded from www.Manualslib.com manuals search engine

clear mobility-domain

Clears all Mobility Domain configuration and information from a WX switch, regardless of whether the WX switch is a seed or a member of a Mobility Domain.

Syntax — **`clear mobility-domain`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command has no effect if the WX switch is not configured as part of a Mobility Domain.

Examples — To clear a Mobility Domain from a WX switch within the domain**,** type the following command:

```
WX1200# clear mobility-domain
success: change accepted.
```

See Also

- **clear mobility-domain member** on page 266
- **set mobility-domain member** on page 269
- **set mobility-domain mode member seed-ip** on page 270
- **set mobility-domain mode seed domain-name** on page 271

clear mobility-domain member

On the seed WX switch, removes the identified member from the Mobility Domain.

Syntax — **`clear mobility-domain member`** *`ip-addr`*

- *`ip-addr`* — IP address of the Mobility Domain member, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — This command has no effect if the WX switch member is not configured as part of a Mobility Domain or the current WX switch is not the seed.

Examples — The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
WX1200# clear mobility-domain member 192.168.0.1
```

See Also

- **set mobility-domain member** on page 269

display mobility-domain config

Displays the configuration of the Mobility Domain.

Syntax — **display mobility-domain config**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays the Mobility Domain configuration:

```
WX4400# display mobility-domain config
This WX is a member, with seed 192.168.14.6
```

See Also

- **clear mobility-domain** on page 266
- **set mobility-domain member** on page 269
- **display mobility-domain status** on page 267

display mobility-domain status

On the seed WX, displays the Mobility Domain status and members.

Syntax — **display mobility-domain status**

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

Examples — To display Mobility Domain status, type the following command:

```
WX4400# display mobility-domain status
Mobility Domain name:  Pleasanton
Member              State             Status
---------------     -------------     --------------
192.168.253.11      STATE_UP          MEMBER
192.168.253.12      STATE_DOWN        MEMBER
192.168.253.14      STATE_UP          SEED
```

Table 46 describes the fields in the display.

Table 46 display mobility-domain Output

Field	Description
Mobility Domain name	Name of the Mobility Domain
Member	IP addresses of the seed WX switch and members in the Mobility Domain
State	State of the WX switch in the Mobility Domain: ▪ STATE_UP ▪ STATE_DOWN
Status	Role of the WX switch in the Mobility Domain: ▪ MEMBER ▪ SEED

See Also

- **clear mobility-domain** on page 266
- **set mobility-domain member** on page 269
- **set mobility-domain mode member seed-ip** on page 270

Downloaded from www.Manualslib.com manuals search engine

set mobility-domain member

On the seed WX switch, adds a member to the list of Mobility Domain members. If the current WX switch is not configured as a seed, this command is rejected.

Syntax — **`set mobility-domain member`** *`ip-addr`*

- *`ip-addr`* — IP address of the Mobility Domain member in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command must be entered from the seed WX switch.

Examples — The following commands add three WX switches with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain whose seed is the current WX switch:

```
WX4400# set mobility-domain member 192.168.1.8
success: change accepted.
WX4400# set mobility-domain member 192.168.1.9
success: change accepted.
WX4400# set mobility-domain member 192.168.1.10
success: change accepted.
```

See Also

- **clear mobility-domain member** on page 266
- **display mobility-domain config** on page 267
- **set mobility-domain mode seed domain-name** on page 271

Downloaded from www.Manualslib.com manuals search engine

set mobility-domain mode member seed-ip

On a nonseed WX switch, sets the IP address of the seed WX switch. This command is used on a member WX to configure it as a member. If the WX switch is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

Syntax — **`set mobility-domain mode member seed-ip`** *`ip-addr`*

- *`ip-addr`* — IP address of the Mobility Domain member, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command sets the current WX switch as a nonseed member of the Mobility Domain whose seed has the IP address 192.168.1.8:

```
WX4400# set mobility-domain mode member seed-ip 192.168.1.8
mode is: member
seed IP is: 192.168.1.8
```

See Also

- **clear mobility-domain** on page 266
- **display mobility-domain config** on page 267

Downloaded from www.Manualslib.com manuals search engine

set mobility-domain mode seed domain-name

Creates a Mobility Domain by setting the current WX switch as the seed device and naming the Mobility Domain.

Syntax — **`set mobility-domain mode seed domain-name`** *`mob-domain-name`*

- *`mob-domain-name`* — Name of the Mobility Domain. Specify between 1 and 16 characters with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Before you use this command, the current WX switch must have its IP address set with the **set system ip-address** command. After you enter this command, all Mobility Domain traffic is sent and received from the specified IP address.

You must explicitly configure *only one* WX switch per domain as the seed. All other WX switches in the domain receive their Mobility Domain information from the seed.

Examples — The following command creates a Mobility Domain named Pleasanton with the current WX switch as the seed:

```
WX4400# set mobility-domain mode seed domain-name Pleasanton
mode is: seed
domain name is: Pleasanton
```

See Also

- **clear mobility-domain member** on page 266
- **display mobility-domain status** on page 267

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

10 Network Domain Commands

Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information among themselves over a WAN link. This shared information allows a user configured on a WX switch in one Mobility Domain to establish connectivity on a WX switch in another Mobility Domain elsewhere in the same Network Domain. The WX switch forwards the user traffic by creating a VLAN tunnel to a WX switch in the remote Mobility Domain.

In a Network Domain, one or more WX switches serve as a seed switch. At least one of the Network Domain seeds maintains a connection with each of the member WX switches in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

Network Domain Commands by Usage

This chapter presents Network Domain commands alphabetically. Use Table 47 to locate commands in this chapter based on their use.

Table 47 Network Domain Commands by Usage

Type	Command
Network Domain	**set network-domain mode seed domain-name** on page 282
	set network-domain mode member seed-ip on page 280
	set network-domain peer on page 281
	clear network-domain on page 274
	clear network-domain mode on page 275

Downloaded from www.Manualslib.com manuals search engine

Table 47 Network Domain Commands by Usage (continued)

Type	Command
	clear network-domain peer on page 276
	clear network-domain seed-ip on page 277
	display network-domain on page 278

clear network-domain

Clears all Network Domain configuration and information from a WX switch, regardless of whether the WX switch is a seed or a member of a Network Domain.

Syntax — `clear network-domain`

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Examples — This command has no effect if the WX switch is not configured as part of a Network Domain.

To clear a Network Domain from a WX switch within the domain**,** type the following command:

```
WX1200# clear network-domain
This will clear all network-domain configuration. Would you
like to continue? (y/n) [n] y
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 280
- **set network-domain peer** on page 281
- **set network-domain mode seed domain-name** on page 282

Downloaded from www.Manualslib.com manuals search engine

clear network-domain mode

Removes the Network Domain seed or member configuration from the WX switch.

Syntax — **`clear network-domain mode {seed | member}`**

- **`seed`** — Clears the Network Domain seed configuration from the WX switch.
- **`member`** — Clears the Network Domain member configuration from the WX switch.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — This command has no effect if the WX switch is not configured as part of a Network Domain.

Examples — The following command clears the Network Domain member configuration from the WX switch:

```
WX1200# clear network-domain mode member
success: change accepted.
```

The following command clears the Network Domain seed configuration from the WX switch:

```
WX1200# clear network-domain mode seed
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 280
- **set network-domain mode seed domain-name** on page 282

Downloaded from www.Manualslib.com manuals search engine

clear network-domain peer

Removes the configuration of a Network Domain peer from a WX switch configured as a Network Domain seed.

Syntax — **`clear network-domain peer {`***`ip-addr`* **`| all}`**

- *`ip-addr`* — IP address of the Network Domain peer in dotted decimal notation.
- **`all`** — Clears the Network Domain peer configuration for all peers from the WX switch.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — This command has no effect if the WX switch is not configured as a Network Domain seed.

Examples — The following command clears the Network Domain peer configuration for peer 192.168.9.254 from the WX switch:

```
WX1200# clear network-domain peer 192.168.9.254
success: change accepted.
```

The following command clears the Network Domain peer configuration for all peers from the WX switch:

```
WX1200# clear network-domain peer all
success: change accepted.
```

See Also

- **set network-domain peer** on page 281

Downloaded from www.Manualslib.com manuals search engine

clear network-domain seed-ip

Removes the specified Network Domain seed from the WX switch's configuration. When you enter this command, the Network Domain TCP connections between the WX switch and the specified Network Domain seed are closed.

Syntax — **`clear network-domain seed-ip`** *`ip-addr`*

- *`ip-addr`* — IP address of the Network Domain seed in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — This command has no effect if the WX switch is not configured as part of a Network Domain, or if the WX switch is not configured as a member of a Network Domain that uses the specified Network Domain seed.

The following command removes the Network Domain seed with IP address 192.168.9.254 from the WX switch's configuration:

```
WX1200# clear network-domain seed-ip 192.168.9.254
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 280

Downloaded from www.Manualslib.com manuals search engine

display network-domain

Displays the status of Network Domain seeds and members.

Syntax — **`display network-domain`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Examples — To display Network Domain status, type the following command. The output of the command differs based on whether the WX switch is a member of a Network Domain or a Network Domain seed.

On a WX switch that is a Network Domain member, the following output is displayed:

```
WX1200# display network-domain
Member Network Domain name: California
Member        State      Mode
------------------     ------
10.8.107.1      UP      SEED
```

On a WX switch that is a Network Domain seed, information is displayed about the Network Domains of which the WX switch is a member, as well as Network Domain seeds with which the WX switch has a peer relationship. For example:

```
WX1200# display network-domain
Network Domain name: California
Peer                State
---------------     -------------
10.8.107.1          UP
Member              State             Mode
---------------    -------------    ------
10.1.0.0            DOWN                SEED
Member Network Domain name:
Member              State             Mode
---------------     -----------     ------
10.8.107.1          UP               MEMBER
10.1.0.0            DOWN             SEED
```

Downloaded from www.Manualslib.com manuals search engine

Table 48 describes the fields in the display.

Table 48 Radio-Specific Parameters

Parameter	Description
Output if WX is the Network Domain Seed	
Network Domain name	Name of the Network Domain for which the WX switch is a seed.
Peer	IP addresses of the other seeds in the Network Domain.
State	State of the connection between the WX switch and the peer Network Domain seeds: ▪ UP ▪ DOWN
Member	IP addresses of the seed WX switch and members in the Network Domain.
State	State of the WX switch in the Network Domain: ▪ UP ▪ DOWN
Mode	Role of the WX switch in the Network Domain: ▪ UP ▪ DOWN
Output if WX is a Network Domain Member	
Member Network Domain name	Name of the Network Domain of which the WX switch is a member.
Member	IP addresses of the seed WX switch and members in the Network Domain.
State	State of the WX switch in the Network Domain. ▪ UP ▪ DOWN
Mode	Role of the WX switch in the Network Domain: ▪ MEMBER ▪ SEED

See Also

- **clear network-domain** on page 274
- **set network-domain mode member seed-ip** on page 280
- **set network-domain mode seed domain-name** on page 282
- **set network-domain peer** on page 281

Downloaded from www.Manualslib.com manuals search engine

set network-domain mode member seed-ip

Sets the IP address of a Network Domain seed. This command is used for configuring a WX switch as a member of a Network Domain. You can specify multiple Network Domain seeds and configure one as the primary seed.

Syntax — **set network-domain mode member seed-ip** *ip-addr* **[affinity** *num***]**

- *ip-addr* — IP address of the Network Domain seed, in dotted decimal notation.
- *num* — Preference for using the specified Network Domain seed. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults — The default affinity for a Network Domain seed is 5.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — You can specify multiple Network Domain seeds on the WX switch. When the WX switch needs to connect to a Network Domain seed, it first attempts to connect to the seed with the highest affinity. If that seed is unavailable, the WX attempts to connect to the seed with the next-highest affinity. After a connection is made to a non-highest-affinity seed, the WX switch then periodically attempts to connect to the highest-affinity seed.

Examples — The following command sets the WX switch as a member of the Network Domain whose seed has the IP address 192.168.1.8:

```
WX1200# set network-domain mode member seed-ip 192.168.1.8
success: change accepted.
```

The following command sets the WX switch as a member of a Network Domain whose seed has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the WX switch specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for this WX switch.

Downloaded from www.Manualslib.com manuals search engine

```
WX1200# set network-domain mode member seed-ip 192.168.9.254
affinity 7
success: change accepted.
```

See Also

- **clear network-domain** on page 274
- **display network-domain** on page 278

---

set network-domain peer

On a Network Domain seed, configures one or more WX switches as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

Syntax — **set network-domain peer** *ip-addr*

- *ip-addr* — IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — This command must be entered on a WX switch configured as a Network Domain seed.

Examples — The following command sets the WX switch with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
WX1200# set network-domain peer 192.168.9.254
success: change accepted.
```

See Also

- **clear network-domain** on page 274
- **display network-domain** on page 278

Downloaded from www.Manualslib.com manuals search engine

set network-domain mode seed domain-name

Creates a Network Domain by setting the current WX switch as a seed device and naming the Network Domain.

Syntax — **`set network-domain mode seed domain-name`** *`net-domain-name`*

- *`net-domain-name`* — Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — Before you use this command, the current WX switch must have its IP address set with the **set system ip-address** command. After you enter this command, Network Domain traffic is sent and received from the specified IP address.

You can configure multiple WX switches as Network Domain seeds. If you do this, you must identify them as peers by using the **set network domain peer** command.

Examples — The following command creates a Network Domain named California with the current WX switch as a seed:

```
WX1200# set network-domain mode seed domain-name California
success: change accepted.
```

The seed switch in a Network Domain must also be configured as a member of the Network Domain, with the specified seed IP address pointing to the seed itself.

`set network-domain mode member seed-ip` *`ip-addr`* **`[affinity`** *`num`***`]`**

For example, the following command sets the current WX switch as a member of a Network Domain where the WX switch with IP address 192.168.9.254 is a seed:

```
WX1200# set network-domain mode member seed-ip 192.168.9.254
success: change accepted.
```

See Also

- **clear network-domain** on page 274
- **display network-domain** on page 278

Downloaded from www.Manualslib.com manuals search engine

11 MANAGED ACCESS POINT COMMANDS

Use MAP access point commands to configure and manage MAP access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the WX switch. (See **set system countrycode** on page 56.)
- Install the MAP access point and connect it to a port on the WX switch.
- Configure a MAP access port (for a directly connected MAP) or a Distributed MAP. (See **set port type ap** on page 91 and **set dap** on page 81.)

CAUTION: *Changing the system country code after MAP configuration disables MAP access points and deletes their configuration. If you change the country code on a WX switch, you must reconfigure all MAP access points.*

MAP Access Point Commands by Usage

This chapter presents MAP access point commands alphabetically. Use Table 49 to locate commands in this chapter based on their use.

Table 49 Map Access Point Commands by Usage

Type	Command
Automatic Configuration of Distributed MAPs	**set dap auto** on page 325
	set dap auto mode on page 327
	set {ap | dap} bias on page 328
	set {ap | dap} blink on page 330
	set {ap | dap} group on page 332
	set {ap | dap} radio auto-tune max-power on page 335
	set {ap | dap} radio auto-tune max- retransmissions on page 337

Downloaded from www.Manualslib.com manuals search engine

Table 49 Map Access Point Commands by Usage (continued)

Type	Command
	set {ap | dap} radio auto-tune min-client-rate on page 340
	set {ap | dap} radio mode on page 341
	set {ap | dap} radio radio-profile on page 343
	set dap auto radiotype on page 326
	set {ap | dap} upgrade-firmware on page 346
External Antenna	**set {ap | dap} radio antennatype** on page 334
Radio Profile Assignment	**set {ap | dap} radio radio-profile** on page 343
	set radio-profile mode on page 362
	clear radio-profile on page 288
	set radio-profile service-profile on page 366
	display radio-profile on page 317
SSID Assignment	**set service-profile ssid-name** on page 384
	set service-profile ssid-type on page 385
	set service-profile beacon on page 376
Radio Properties	**set radio-profile 11g-only** on page 347
	set radio-profile beacon-interval on page 355
	set radio-profile rts-threshold on page 365
	set radio-profile frag-threshold on page 358
	set radio-profile short-retry on page 369
	set radio-profile long-retry on page 359
	set radio-profile max-rx-lifetime on page 360
	set radio-profile max-tx-lifetime on page 361
	set radio-profile preamble-length on page 364
	set radio-profile countermeasures on page 355
	set radio-profile active-scan on page 348
	set radio-profile wmm on page 370
Authentication and Encryption	**set service-profile attr** on page 371
	set service-profile auth-dot1x on page 373
	set service-profile auth-fallthru on page 374
	set service-profile web-portal-form on page 387
	set service-profile auth-psk on page 375

Downloaded from www.Manualslib.com manuals search engine

Table 49 Map Access Point Commands by Usage (continued)

Type	Command
	set service-profile wpa-ie on page 391
	set service-profile rsn-ie on page 383
	set service-profile cipher-ccmp on page 377
	set service-profile cipher-tkip on page 378
	set service-profile cipher-wep104 on page 379
	set service-profile cipher-wep40 on page 380
	set service-profile psk-phrase on page 381
	set service-profile psk-raw on page 382
	set service-profile tkip-mc-time on page 386
	set service-profile wep active-multicast- index on page 388
	set service-profile wep active-unicast- index on page 389
	set service-profile wep key-index on page 390
	set service-profile shared-key-auth on page 384
	display service-profile on page 321
	clear service-profile on page 289
RF Auto-Tuning	**set radio-profile auto-tune channel-config** on page 349
	set radio-profile auto-tune channel-holddown on page 350
	set radio-profile auto-tune channel-interval on page 351
	set radio-profile auto-tune power-backoff- timer on page 352
	set radio-profile auto-tune power-config on page 353
	set radio-profile auto-tune power-interval on page 354
	set {ap | dap} radio auto-tune max-power on page 335
	set {ap | dap} radio auto-tune max- retransmissions on page 337
	set {ap | dap} radio auto-tune min-client-rate on page 340
	display auto-tune neighbors on page 311
	display auto-tune attributes on page 309

Downloaded from www.Manualslib.com manuals search engine

Table 49 Map Access Point Commands by Usage (continued)

Type	Command
MAP-WX Security	**set dap fingerprint** on page 331
	set dap security on page 345
Radio State	**set {ap | dap} radio mode** on page 341
Dual Homing	**set {ap | dap} bias** on page 328
Load Balancing	**set {ap | dap} group** on page 332
	display {ap | dap} group on page 303
MAP Administration and Maintenance	**set {ap | dap} name** on page 333
	set {ap | dap} blink on page 330
	set {ap | dap} upgrade-firmware on page 346
	reset {ap | dap} on page 324
	set {ap | dap} radio channel on page 339
	set {ap | dap} radio tx-power on page 344
	clear {ap | dap} radio on page 286
	display {ap | dap} group on page 303
	display {ap | dap} status on page 304
	display {ap | dap} counters on page 294
	display dap global on page 314
	display dap connection on page 313
	display dap unconfigured on page 316
	display {ap | dap} qos-stats on page 300
	display {ap | dap} etherstats on page 301

clear {ap | dap} radio

Disables a MAP radio and resets it to its factory default settings.

Syntax — **clear** {**ap** *port-list* | **dap** *dap-num* } **radio** {**1** | **2** | **all**}

- **ap** *port-list* — List of ports connected to the MAP access point(s) on which to reset a radio.
- **dap** *dap-num* — Number of a Distributed MAP on which to reset a radio.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **radio all** — All radios on the MAP.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The **clear ap radio** command resets the radio to the default settings listed in Table 50 and in Table 66 on page 362.

Table 50 Radio-Specific Parameters

Parameter	Default Value	Description
channel	▪ **802.11b** — 6 ▪ **802.11a** — Lowest valid channel number for the country of operation	Number of the channel in which a radio transmits and receives traffic
tx-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	Transmit power of a radio, in decibels referred to 1 milliwatt (dBm)
antennatype	For most MAP models, the default is **internal**. For MP-620, the default for the 802.11b/g radio is ANT-1360-OUT. The default for the 802.11a radio is ANT-5360 OUT. The default for the 802.11b/g radio on model MP-262 is ANT1060.	External antenna model Note: This parameter is configurable only on MAPs that support external antennas.

Access — Enabled

History —Introduced in MSS Version 3.0.

Usage — When you clear a radio, MSS performs the following actions:

- Clears the transmit power, channel, and external antenna setting from the radio.
- Removes the radio from its radio profile and places the radio in the *default* radio profile.

This command does not affect the PoE setting.

Examples — The following command disables and resets radio 2 on the MAP access point connected to port 3:

```
WX1200# clear ap 3 radio 2
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set {ap | dap} radio mode** on page 341
- **set {ap | dap} radio radio-profile** on page 343
- **set port type ap** on page 91

clear radio-profile

Removes a radio profile or resets one of the profile's parameters to its default value.

Syntax — **clear radio-profile** *name* [*parameter*]

- *name* — Radio profile name.
- *parameter* — Radio profile parameter:
  - **beacon-interval**
  - **dtim-interval**
  - **frag-threshold**
  - **long-retry**
  - **max-rx-lifetime**
  - **max-tx-lifetime**
  - **preamble-length**
  - **rts-threshold**
  - **service-profile**
  - **short-retry**

  (For information about these parameters, see the **set radio-profile** commands that use them.)

Defaults — If you reset an individual parameter, the parameter is returned to the default value listed in Table 66 on page 362.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you specify a parameter, the setting for the parameter is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands disable the radios that are using radio profile *rp1* and reset the **beaconed-interval** parameter to its default value:

```
WX4400# set radio-profile rp1 mode disable
WX4400# clear radio-profile rp1 beacon-interval
success: change accepted.
```

The following commands disable the radios that are using radio profile *rptest* and remove the profile:

```
WX4400# set radio-profile rptest mode disable
WX4400# clear radio-profile rptest
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set {ap | dap} radio radio-profile** on page 343
- **set radio-profile mode** on page 362

---

clear service-profile

Removes a service profile or resets one of the profile's parameters to its default value.

Syntax — **clear service-profile** *name*

- *name* — Service profile name.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile** *name* **service-profile** *name* command.)

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands disable the radios that are using radio profile *rp6*, remove service-profile *svcprof6* from *rp6*, then clear *svcprof6* from the configuration.

```
WX4400# set radio-profile rp6 mode disable
WX4400# clear radio-profile rp6 service-profile svcprof6
success: change accepted.
WX4400# clear service-profile svcprof6
success: change accepted.
```

See Also

- **clear radio-profile** on page 288
- **set radio-profile mode** on page 362

display {ap | dap} config

Displays global and radio-specific settings for a MAP access point.

Syntax — **display ap config** [*port-list* [**radio** {**1** | **2**}]]

Syntax — **display dap config** [*dap-num* [**radio** {**1** | **2**}]]

- *port-list* — List of ports connected to the MAP access point(s) for which to display configuration settings.
- *dap-num* — Number of a Distributed MAP for which to display configuration settings.
- **radio 1** — Shows configuration information for radio 1.
- **radio 2** — Shows configuration information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Usage — MSS lists information separately for each MAP access point.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example shows configuration information for a MAP access point on WX port 2:

```
WX1200# display ap config 2
Port  1: AP model: AP2750, POE:  enable, bias: high, name: MAP01
          boot-download-enable: YES
          load balancing group: none
  Radio 1: type: 802.11g, mode:  enabled, channel: dynamic
  tx pwr: dynamic, profile: default
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
```

The following example shows configuration information for a Distributed MAP access point configured on connection 1:

```
WX4400# display dap config 1
Dap  1: Serial-Id: M9DE48B012F00, MAP model: AP2750, bias: high, name: DAP1
          boot-download-enable: YES
  Radio 1: type: 802.11a, mode: disabled, channel: dynamic
  tx pwr: 11, profile: default
  auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

Table 51 describes the fields in this display.

Table 51 Output for display ap config

Field	Description
Port	WX port number. **Note:** This field is applicable only if the MAP is directly connected to the WX switch and the WX switch's port is configured as a MAP access port.
DAP	Connection ID for the Distributed MAP. **Note:** This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.
Serial-Id	Serial ID of the MAP access point. **Note:** This field is displayed only for Distributed MAPs.
AP model	MAP access point model number.
POE	PoE state on the WX port: ▪ Enable ▪ Disable
bias	Bias of the WX connection to the MAP: ▪ High ▪ Low

Downloaded from www.Manualslib.com manuals search engine

Table 51 Output for display ap config (continued)

Field	Description
name	MAP access point name.
boot-download-enable	State of the firmware upgrade option: ■ YES (automatic upgrades are enabled) ■ NO (automatic upgrades are disabled)
load balancing group	Names of the MAP load-balancing groups to which the MAP access point belongs. If the value is *None*, the access point does not belong to any load balancing groups. **Note:** This field is displayed only if the MAP is a member of a group.
Radio	Radio number. The information listed below this field applies specifically to the radio.
type	Radio type: ■ 802.11a ■ 802.11b ■ 802.11g
mode	Radio state: ■ Enabled ■ Disabled
channel	Channel number.
antennatype	External antenna model, if applicable.
tx pwr	Transmit power, in dBm.
profile	Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS assigns the radio to the default radio profile.
auto-tune max-power	Maximum power level the RF Auto-Tuning feature can set on the radio. ■ The value default means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation. ■ A specific numeric value means you or another administrator set the maximum value.
auto-tune min-client-rate	Minimum data rate the radio must maintain for associated clients. When RF Auto-Tuning is enabled, the radio can temporarily increase its power to maintain the data rate with an associated client.

Downloaded from www.Manualslib.com manuals search engine

Table 51 Output for display ap config (continued)

Field	Description
auto-tune max-retransmissions	Maximum percentage of packets that can be retransmitted by a client before RF Auto-Tuning increases power. **Note:** Only packets that are received twice by the MAP are counted as retransmissions. If a client retransmits a packet but the MAP receives only a single copy of the packet, the packet is not counted as a retransmission.

See Also

- **display dap connection** on page 313
- **display dap global** on page 314
- **display dap unconfigured** on page 316
- **display radio-profile** on page 317
- **set dap** on page 81
- **set port type ap** on page 91
- **set {ap | dap} bias** on page 328
- **set {ap | dap} group** on page 332
- **set {ap | dap} name** on page 333
- **set {ap | dap} upgrade-firmware** on page 346
- **set {ap | dap} radio mode** on page 341
- **set {ap | dap} radio antennatype** on page 334
- **set {ap | dap} radio channel** on page 339
- **set {ap | dap} radio radio-profile** on page 343
- **set {ap | dap} radio tx-power** on page 344

Downloaded from www.Manualslib.com manuals search engine

display {ap | dap} counters

Displays MAP access point and radio statistics counters.

Syntax — **display ap counters** [*port-list* [**radio** {**1** | **2**}]]

Syntax — **display dap counters** [*dap-num* [**radio** {**1** | **2**}]]

- *port-list* — List of ports connected to the MAP access point(s) for which to display statistics counters.
- *dap-num* — Number of a Distributed MAP for which to display statistics counters.
- **radio 1** — Shows statistics counters for radio 1.
- **radio 2** — Shows statistics counters for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0. New fields added in MSS Version 4.0:

- Radio Recv Phy Err Ct
- Transmit Retries
- Radio Adjusted Tx Pwr
- Noise Floor
- 802.3 Packet Tx Ct
- 803.3 Packet Rx Ct
- No Receive Descriptor

Usage — To display statistics counters and other information for individual user sessions, use the **display sessions network** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows statistics counters for Distributed MAP 7:

```
WX1200# display dap counters 7
Port: 6                radio: 1
================================
LastPktXferRate        2         PktTxCount         91594255
NumCntInPwrSave        4294966683MultiPktDrop       0
LastPktRxSigStrength   -54       MultiBytDrop       0
LastPktSigNoiseRatio   40        User Sessions      5
TKIP Pkt Transfer Ct   0         MIC Error Ct       0
TKIP Pkt Replays       0         TKIP Decrypt Err   0
CCMP Pkt Decrypt Err   0         CCMP Pkt Replays   0
CCMP Pkt Transfer Ct   0         RadioResets        0
Radio Recv Phy Err Ct  0         Transmit Retries   60501
Radio Adjusted Tx Pwr  15        Noise Floor        -93
802.3 Packet Tx Ct     0         802.3 Packet Rx Ct 0
No Receive Descriptor  0
```

```
     TxUniPkt     TxUniByte        RxPkt  RxByte   UndcrptPkt
            TxMultiPkt     TxMultiByte                  UndcrptByte
                                                             PhyError
 1.0: 164492     0  9631741       0 405041  8913512    0    0 13963
 2.0:    603     0   248716       0 191103  4608065    0    0 30547
 5.5: 370594 52742 27616521 4445625   2427   133217    0    0   723
 6.0:    0     0      0       0    0     0    0    0    51
 9.0:    0     0      0       0    1   172    0    0    53
11.0:   8016     0  2590353       0  85479  3897587    0    0  1195
12.0:    0     0      0       0    0     0    0    0    26
18.0:    0     0      0       0    0     0    0    0    38
24.0:    0     0      0       0    0     0    0    0    47
36.0:    0     0      0       0    0     0    0    0     1
48.0:    0     0      0       0    1    68    0    0    29
54.0:    0     0      0       0    0     0    0    0     5

TOTL: 543705 52742 40087331 4445625 684050 17552381    0    0 46441
```

Downloaded from www.Manualslib.com manuals search engine

Table 52 describes the fields in this display.

Table 52 Output for display ap counters

Field	Description
DAP	Distributed MAP number.
Port	WX port number (if the MAP is directly connected to the WX and the WX port is configured as a MAP access point).
radio	Radio number.
LastPktXferRate	Data transmit rate, in Mbps, of the last packet received by the MAP access point.
NumCntInPwrSave	Number of clients currently in power save mode.
LastPktRxSigStrength	Signal strength, in dBm, of the last packet received by the MAP access point.
LastPktSigNoiseRatio	Signal-to-noise ratio, in decibels (dB), of the last packet received by the MAP access point. This value indicates the strength of the radio signal above the noise floor. For example, if the noise floor is -88 and the signal strength is -68, the SNR is 20. If the value is below 10, this indicates a weak signal and might indicate a problem in the RF environment.
TKIP Pkt Transfer Ct	Total number of TKIP packets sent and received by the radio.
TKIP Pkt Replays	Number of TKIP packets that were resent to the MAP by a client. A low value (under about one hundred) does not necessarily indicate a problem. However, if this counter is increasing steadily or has a very high value (in the hundreds or more), a Denial of Service (DoS) attack might be occurring. Contact 3Com TAC.
CCMP Pkt Decrypt Err	Number of times a decryption error occurred with a packet encrypted with CCMP. Occasional decryption errors do not indicate a problem. However, steadily increasing errors or a high number of errors can indicate that data loss is occurring in the network. Generally, this is caused by a key mismatch between a client and the MAP. To locate the client that is experiencing decryption errors (and therefore is likely causing this counter to increment on the MAP), use the **display sessions network session-id session-id** command for each client on the radio. After you identify the client that is causing the errors, disable and reenable the client (wireless NIC).

Downloaded from www.Manualslib.com manuals search engine

Table 52 Output for display ap counters (continued)

Field	Description
CCMP Pkt Transfer Ct	Total number of CCMP packets sent and received by the radio.
Radio Recv Phy Err Ct	Number of times radar caused packet errors. If this counter increments rapidly, there is a problem in the RF environment. This counter increments only when radar is detected. Rate-specific Phy errors are instead counted in the PhyError columns for individual data rates.
Radio Adjusted Tx Pwr	Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level.
802.3 Packet Tx Ct	Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
No Receive Descriptor	Number of packets for which the MAP could not create a descriptor. A descriptor describes a received packet's size and its location in MAP memory. The MAP buffers descriptors, and clears them during interframe spaces. This counter increments if the MAP runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the MAP attempts to buffer the noise as packets. Buffer overruns are normal while a MAP is booting. However, if they occur over an extended period of time when the MAP is fully active, this can indicate RF interference.
PktTxCount	Number of packets transmitted by the radio.
MultiPktDrop	Number of multicast packets dropped by the radio due to a buffer overflow on the MAP. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0.
MultiBytDrop	Number of multicast bytes dropped by the radio due to a buffer overflow on the MAP. (See the description for MultiPktDrop.)

Downloaded from www.Manualslib.com manuals search engine

Table 52 Output for display ap counters (continued)

Field	Description
User Sessions	Number of clients currently associated with the radio. Generally, this counter is equal to the number of sessions listed for the radio in **display sessions** output. However, the counter can differ from the counter in **display sessions** output if a client is associated with the radio but has not yet completed 802.1X authentication. In this case, the client is counted by this counter but not in the **display sessions** output. Although there is no specific normal range for this counter, a high or low number relative to other radios can mean the radio is underutilized or overutilized relative to the other radios. (However, if the clients are VoIP phones, a relatively high number of clients does not necessarily mean overutilization since voice clients consume less bandwidth on average than data clients.)
MIC Error Ct	Number of times the radio received a TKIP-encrypted frame with an invalid MIC. Normally, the value of this counter should always be 0. If the value is not 0, check the system log for MIC error messages and contact 3Com TAC.
TKIP Decrypt Err	Number of times a decryption error occurred with a packet encrypted with TKIP. (See the description for CCMP Pkt Decrypt Err.)
CCMP Pkt Replays	Number of CCMP packets that were resent to the MAP by a client. (See the description for TKIP Pkt Replays.)
RadioResets	Number of times the radio has been reset. Generally, a reset occurs as a result of RF noise. It is normal for this counter to increment a few times per day.
Transmit Retries	Number of times the radio retransmitted a unicast packet because it was not acknowledged. The MAP uses this counter to adjust the transmit data rate for a client, in order to minimize retries. The ratio of transmit retries to transmitted packets (TxUniPkt) indicates the overall transmit quality. A ratio of about 1 retry to 10 transmitted packets indicates good transmit quality. A ratio of 3 or more to 10 indicates poor transmit quality. This counter includes unacknowledged probes. Some clients do not respond to probes, which can make this counter artificially high.

Downloaded from www.Manualslib.com manuals search engine

Table 52 Output for display ap counters (continued)

Field	Description
Noise Floor	Received signal strength at which the MAP can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference.
802.3 Packet Rx Ct	Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
The counters above are global for all data rates. The counters below are for individual data rates. If counters for lower data rates are incrementing but counters for higher data rates are not incrementing, this can indicate poor throughput. The poor throughput can be caused by interference. If the cause is not interference or the interference cannot be eliminated, you might need to relocate the MAP in order to use the higher data rates and therefore improve throughput.	
TxUniPkt	Number of unicast packets transmitted by the radio..
TxMultiPkt	Number of multicast packets transmitted by the radio.
TxUniByte	Number of unicast bytes transmitted by the radio.
TxMultiByte	Number of multicast bytes transmitted by the radio.
RxPkt	Number of packets received by the radio.
RxByte	Number of bytes received by the radio.
UndcrptPkt	Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network..
UndcrptByte	Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.)
PhyError	Number of packets that could not be decoded by the MAP. This condition can have any of the following causes: ■ Collision of an 802.11 packet. ■ Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the MAP. ■ Interference caused by an 802.11b/g phone or other source. It is normal for this counter to be about 10 percent of the total RxByte count. It is also normal for higher data rates to have higher Phy error counts than lower data rates.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display sessions network** on page 525

---

display {ap | dap} qos-stats

Displays statistics for MAP forwarding queues.

Syntax — **display dap qos-stats [***dap-num***]**

Syntax — **display ap qos-stats [***port-list***]**

- *dap-num* — Number of a Distributed MAP for which to display QoS statistics counters.
- *port-list* — List of ports connected to the MAP access point(s) for which to display QoS statistics counters.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command shows statistics for the MAP forwarding queues on a Distributed MAP:

```
WX4400# display dap qos-stats 4

CoS   Queue      Tx
==========================
    DAP: 4 radio: 1
1,2   Background         19
0,3   BestEffort        437
4,5   Video             3034
6,7   Voice             3068

CoS   Queue      Tx
==========================
    DAP: 4 radio: 2
1,2   Background         11
0,3   BestEffort        221
4,5   Video             3631
6,7   Voice             7892
```

Downloaded from www.Manualslib.com manuals search engine

Table 53 describes the fields in this display.

Table 53 Output for display {ap | dap} qos-stats

Field	Description
CoS	CoS value associated with the forwarding queues.
Queue	Forwarding queue.
DAP or Port	Distributed MAP number or MAP port number.
radio	Radio number.
Tx	Number of packets transmitted to the air from the queue.

display {ap | dap} etherstats

Displays Ethernet statistics for a MAP's Ethernet ports.

Syntax — **`display`** {**`ap`** | **`dap`**} **`etherstats`** [*`port-list`* | *`dap-num`*]

- *`port-list`* — List of WX switch ports directly connected to the MAPs for which to display counters.
- *`dap-num`* — Number of a Distributed MAP for which to display counters.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays Ethernet statistics for the Ethernet ports on Distributed MAP 1:

```
WX4400# display dap etherstats 1
DAP: 1                ether: 1
================================
RxUnicast:          75432   TxGoodFrames:       55210
RxMulticast:        18789   TxSingleColl:          32
RxBroadcast:            8   TxLateColl:             0
RxGoodFrames:       94229   TxMaxColl:              0
RxAlignErrs:            0   TxMultiColl:           47
RxShortFrames:          0   TxUnderruns:            0
RxCrcErrors:            0   TxCarrierLoss:          0
RxOverruns:             0   TxDeferred:           150
RxDiscards:             0
```

Downloaded from www.Manualslib.com manuals search engine

Table 54 describes the fields in this display.

Table 54 Output of display ap etherstats

Field	Description
RxUnicast	Number of unicast frames received.
RxMulticast	Number of multicast frames received.
RxBroadcast	Number of broadcast frames received.
RxGoodFrames	Number of frames received properly from the link.
RxAlignErrs	Number of received frames that were both misaligned and contained a CRC error.
RxShortFrames	Number of received frames that were shorter than the minimum frame length.
RxCrcErrors	Number of received frames that were discarded due to CRC errors.
RxOverruns	Number of frames known to be lost due to a temporary lack of hardware resources.
RxDiscards	Number of frames known to be lost due to a temporary lack of software resources.
TxGoodFrames	Number of frames transmitted properly on the link.
TxSingleColl	Number of transmitted frames that encountered a single collision.
TxLateColl	Number of frames that were not transmitted because they encountered a collision outside the normal collision window.
TxMaxColl	Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network.
TxMultiColl	Number of transmitted frames that encountered more than one collision.
TxUnderruns	Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources.
TxCarrierLoss	Number of frames transmitted despite the detection of a deassertion of CRS during the transmission.
TxDeferred	Number of frames deferred before transmission due to activity on the link.

Downloaded from www.Manualslib.com manuals search engine

display {ap | dap} group

Displays configuration information and load-balancing status for MAP access point groups.

Syntax — **display** {**ap** | **dap**} **group** [*name*]

- *name* — Name of a MAP group or Distributed MAP group.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays information for MAP access point group *loadbalance1*:

```
WX1200# display ap group loadbalance1

Load Balance Grp Port Clients   Status    Refused
---------------- ---- -------   --------- -------
    loadbalance1    1       1   Accepting       0
    loadbalance1    6       6   Refusing        2
```

Table 55 describes the fields in this display.

Table 55 Output for display ap group

Field	Description
Load Balance Grp	Name of the MAP access point group.
Port	WX port number.
Clients	Number of active client sessions on the MAP access point.
Status	Association status of the MAP access point: ▪ **Accepting** — The MAP access point is accepting new associations. ▪ **Refusing** — The MAP access point is refusing new associations.
Refused	Number of association requests refused by the MAP access point due to load balancing. MSS resets this counter to 0 when the WX switch is restarted, MSS is reloaded, or the access point is removed from the group.

See Also

- **set {ap | dap} group** on page 332

Downloaded from www.Manualslib.com manuals search engine

display {ap | dap} status

Displays MAP access point and radio status information.

Syntax — **display ap status [terse]** [*port-list* | **all** [**radio** {**1** | **2**}]]

Syntax — **display dap status [terse]** [*dap-num* [**radio** {**1** | **2**}]]

- **terse** — Displays a brief line of essential status information for each MAP.
- *port-list* — List of ports connected to the MAP access point(s) for which to display status.
- *dap-num* — Number of a Distributed MAP for which to display status.
- **all** — Shows status information for all directly attached MAP access points and all Distributed MAP access points configured on the switch.
- **radio 1** — Shows status information for radio 1.
- **radio 2** — Shows status information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. True base MAC addresses of radios are displayed in MSS Version 3.2. Previously, the base MAC address displayed for a radio was the true base MAC address plus 2. Note that a radio's base MAC address is also used as the BSSID of the first SSID configured on the radio. New option added: terse; new option added for **display dap status: all**; new field added: fingerprint; MAP-WX security status added to State field in MSS Version 4.0. External antenna information added after the radio state information, to indicate when an antenna has been detected and to indicate the configured antenna model number; *auto* flag added to indicate operational channel or power settings that are configured by RF Auto-Tuning in MSS Version 4.1.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays the status of a Distributed MAP:

```
WX4400# display dap status 1
Dap: 1, IP-addr: 10.2.34.56 (vlan 'vlan-corp'), MAP model: AP2750,
        manufacturer: 3Com, name: DAP01
       fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
==================================================
State:     operational
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                id=0x28f10158a47f0408 ram=33554432
                s/n=0332600444 hw_rev=A3
Uptime:    21 hours, 27 minutes, 51 seconds

Radio 1 type: 802.11g, state: configure succeed [Enabled]
      operational channel: 64 operational power: 14
      base mac: 00:0b:0e:00:d2:c1
      bssid1: 00:0b:0e:00:d2:94, ssid: private
```

The following command displays the status of a directly connected MAP:

```
WX1200# display ap status 1
Port: 1, AP model: AP2750, manufacturer 3Com, name: MAP01
==================================================
State:     operational
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                id=0x28b08a1e047f1d0f ram=33554432
                s/n=0333000288 hw_rev=A3
Uptime:    3 hours, 44 minutes, 28 seconds

Radio 2 type: 802.11g, state: configure succeed [Enabled] (802.11b protect)
      operational channel: 1 operational power: 15
      base mac: 00:0b:0e:00:d1:00
      bssid1: 00:0b:0e:00:d1:00, ssid: public
      bssid2: 00:0b:0e:00:d1:02, ssid: employee-net
      bssid3: 00:0b:0e:00:d1:04, ssid: mycorp-tkip
```

Downloaded from www.Manualslib.com manuals search engine

The following command uses the **terse** option to display brief information for Distributed MAPs:

```
WX4400# display dap status terse
Total number of entries: 4
Operational: 1, Image Downloading: 0, Unknown: 3, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto DAP, i = insecure
Port   Flg IP Address      Model  MAC Address       Radio1 Radio2 Uptime
------ --- ------------- ------ ----------------- ------ ------ ------------
     3 ---               MP-372                   D ?/?  D ?/?   0d 0h 0m 0s
Dap  1 ---               MP-372                   D ?/?  D ?/?   0d 0h 0m 0s
Dap  2 ---               MP-372                   D ?/?  D ?/?   0d 0h 0m 0s
Dap100 oa- 10.8.255.11   MP-122 00:0b:0e:da:da:82 E 1/17 E36/11  0d 0h 0m17s
```

Table 56 and Table 57 describe the fields in this display.

Table 56 Output for display ap status

Field	Description
DAP	Connection ID for the Distributed MAP. **Note:** This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.
Port	WX port number. **Note:** This field is applicable only if the MAP is directly connected to the WX switch and the WX switch's port is configured as a MAP access port.
IP-addr	IP address of the MAP. The address is assigned to the MAP by a DHCP server. **Note:** This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.
AP model	MAP access point model number.
manufacturer	Company that made the MAP access point.
fingerprint	Hexadecimal fingerprint of the MAP's public encryption key. This field is displayed only for Distributed MAPs.
name	MAP access point name.
Link	Status of this link with the MAP access point and the MAP port at the other end of the link. The status can be up or down.

Downloaded from www.Manualslib.com manuals search engine

Table 56 Output for display ap status (continued)

Field	Description
MAP port	MAP port number connected to this WX port.
State	State of the MAP: ▪ **init** — The MAP has been recognized by the WX but has not yet begun booting. ▪ **booting** — The MAP has asked the WX for a boot image. ▪ **image downloading** — The MAP is receiving a boot image from the WX. ▪ **image downloaded** — The MAP has received a boot image from the WX and is booting. ▪ **configuring** — The MAP has booted and is ready to receive or is already receiving configuration parameters from the WX. ▪ **operational** — The MAP has received configuration parameters for one or more radios and is ready to accept client connections. ▪ **configure failure** — One or more of the radio parameters received from the WX is invalid. For Distributed MAPs, this field also indicates whether the MAP's management traffic with the WX is encrypted, and whether the MAP's fingerprint has been verified on the WX: ▪ not encrypted—The management session is not encrypted. ▪ encrypted but fingerprint not verified—The MAP's management traffic is encrypted, but the MAP's fingerprint has not been verified in MSS. ▪ encrypted and verified—The MAP's management traffic is encrypted and the MAP's fingerprint has been verified in MSS.
CPU info	Specifications and identification of the CPU. For MAP models MP-352, MP-341, and MP-52, the ID portion of this field is not applicable.
Uptime	Amount of time since the MAP last rebooted using this link. **Note:** This field is displayed only when this link is the MAP access point's primary link.

Downloaded from www.Manualslib.com manuals search engine

Table 56 Output for display ap status (continued)

Field	Description
Radio 1 type	802.11 type and configuration state of the radio.
Radio 2 type	▪ The *configure succeed* state indicates that the MAP has received configuration parameters for the radio and the radio is ready to accept client connections. ▪ *802.11b protect* indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio. ▪ *Sweep Mode* indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection. ▪ *Countermeasures Enabled* indicates that the radio is sending countermeasures packets to combat a rogue. ▪ The following information appears for external antennas: *External antenna detected, configured as* ***antenna-model***—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (MSS does not detect the specific model.) *External antenna detected, not configured*—Indicates that an external antenna was detected but no external antenna is configured on the radio. *External antenna not detected, configured as* ***antenna-model***—Indicates that an external antenna is configured on the radio but no external antenna was detected.
operational channel	The channel on which the radio is currently operating. If the channel number is followed by *(Auto)*, the value was set by RF Auto-Tuning.
operational power	The power level at which the radio is currently operating. If the power setting is followed by *(Auto)*, the value was set by RF Auto-Tuning.
base mac	Base MAC address of the radio.
bssid, ssid	SSIDs configured on the radio and their BSSIDs.

Downloaded from www.Manualslib.com manuals search engine

Table 57 Output for display ap status terse and display dap status terse

Field	Description
Port	WX port number connected to the MAP.
Flg	Operational status flags for the MAP. For flag definitions, see the key in the command output.
IP Address	IP address of the MAP. The address is assigned to the MAP by a DHCP server. This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.
Model	MAP model number.
MAC Address	MAC address of the MAP.
Radio1	State, channel, and power information for radio 1: The state can be D (disabled) or E (enabled). The channel and power settings are shown as *channel/power*.
Radio2	State, channel, and power information for radio 2.
Uptime	Amount of time since the MAP booted using this link.

display auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

Syntax — **`display auto-tune attributes`**
`[`**`ap`** *`map-num`* `[`**`radio`** `{`**`1`** `|` **`2`** `|` **`all`**`}]]`

Syntax — **`display auto-tune attributes`**
`[`**`dap`** *`dap-num`* `[`**`radio`** `{`**`1`** `|` **`2`** `|` **`all`**`}]]`

- *`map-num`* — MAP port connected to the MAP access point for which to display RF attributes.
- *`dap-num`* — Number of a Distributed MAP for which to display RF attributes.
- **`radio 1`** — Shows RF attribute information for radio 1.
- **`radio 2`** — Shows RF attribute information for radio 2. (This option does not apply to single-radio models.)
- **`radio all`** — Shows RF attribute information for both radios.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command displays RF attribute information for radio 1 on the directly connected MAP access point on port 2:

```
WX1200# display auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
 Noise:                   -92 Packet Retransmission Count:          0
 Utilization:               0 Phy Errors Count:                     0
 CRC Errors count:        122
```

Table 58 describes the fields in this display.

Table 58 Output for display auto-tune attributes

Field	Description
Noise	Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels.
Utilization	Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is.
CRC Errors count	Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference.
Packet Retransmission Count	Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the MAP radio.
Phy Errors Count	Number of frames received by the MAP radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device.

See Also

- **display auto-tune neighbors** on page 311
- **display radio-profile** on page 317
- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune channel-config** on page 349
- **set radio-profile auto-tune channel-holddown** on page 350

Downloaded from www.Manualslib.com manuals search engine

- **set radio-profile auto-tune channel-interval** on page 351
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354

display auto-tune neighbors

Displays the other 3Com radios and third-party 802.11 radios that a 3Com radio can hear.

Syntax — **`display auto-tune neighbors`**
[**`ap`** *`map-num`* [**`radio`** {**`1`** | **`2`**| **`all`**}]]

Syntax — **`display auto-tune neighbors`**
[**`dap`** *`dap-num`* [**`radio`** {**`1`** | **`2`**| **`all`**}]]

- *`map-num`* — MAP port connected to the MAP access point for which to display neighbors.
- *`dap-num`* — Number of a Distributed MAP for which to display neighbors.
- **`radio 1`** — Shows neighbor information for radio 1.
- **`radio 2`** — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)
- **`radio all`** — Shows neighbor information for both radios.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — For simplicity, this command displays a single entry for each 3Com radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if a radio's SSIDs are unadvertised, 3Com radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays neighbor information for radio 1 on the directly connected MAP access point on port 2:

```
WX1200# display auto-tune neighbors ap 2 radio 1
Total number of entries for port 2 radio 1: 5
Channel Neighbor BSS/MAC  RSSI
------- ----------------- ----
      1 00:0b:85:06:e3:60  -46
      1 00:0b:0e:00:0a:80  -78
      1 00:0b:0e:00:d2:c0  -74
      1 00:0b:85:06:dd:00  -50
      1 00:0b:0e:00:05:c1  -72
```

Table 59 describes the fields in this display.

Table 59 Output for display auto-tune neighbors

Field	Description
Channel	Channel on which the BSSID is detected.
Neighbor BSS/MAC	BSSID detected by the radio.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.

See Also

- **display auto-tune attributes** on page 309
- **display radio-profile** on page 317
- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune channel-config** on page 349
- **set radio-profile auto-tune channel-holddown** on page 350
- **set radio-profile auto-tune channel-interval** on page 351
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354

Downloaded from www.Manualslib.com manuals search engine

display dap connection

Displays the system IP address of the WX switch that booted a Distributed MAP.

Syntax — **`display dap connection`**
[*`dap-num`* | **`serial-id`** *`serial-ID`*]

- *`dap-num`* — Number of a Distributed MAP for which to display information about its active connection.
- **`serial-id`** *`serial-ID`* — MAP access point serial ID.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The **serial-id** parameter displays the active connection for the specified Distributed MAP even if that MAP is not configured on this WX switch. If you instead use the command with the *dap-num* parameter or without a parameter, connection information is displayed only for Distributed MAPs that are configured on this WX switch.

This command provides information only if the Distributed MAP is configured on the switch where you use the command. The switch does not need to be the one that booted the MAP, but it must have the MAP in its configuration. Also, the switch that booted the MAP must be in the same Mobility Domain as the switch where you use the command.

If a Distributed MAP is configured on this WX switch (or another WX switch in the same Mobility Domain) but does not have an active connection, the command does not display information for the MAP. To show connection information for Distributed MAPs, use the **display dap global** command on one of the switches where the MAPs are configured.

Examples — The following command displays information for all Distributed MAPs configured on this WX switch that have active connections:

```
WX1200# display dap connection
Total number of entries: 2
DAP Serial Id     DAP IP Address  WX IP Address
--- -----------   --------------- ---------------
2   M9DE48B012F00 10.10.2.27      10.3.8.111
4   M9DE48B123400 10.10.3.34      10.3.8.111
```

Downloaded from www.Manualslib.com manuals search engine

The following command displays connection information specifically for a Distributed MAP with serial ID *M9DE48B6EAD00*:

```
WX1200# display dap connection serial-id M9DE48B6EAD00
Total number of entries: 1
DAP Serial Id     DAP IP Address  WX IP Address
--- -----------   --------------- ---------------
9   M9DE48B6EAD00 10.10.4.88      10.9.9.11
```

Table 60 describes the fields in this display.

Table 60 Output of display dap connection

Field	Description
DAP	Connection ID you assigned to the Distributed MAP. If the connection is configured on another WX switch, this field contains a hyphen (-).
Serial Id	Serial ID of the Distributed MAP.
DAP IP Address	IP address assigned by DHCP to the Distributed MAP.
WX IP Address	System IP address of the WX switch on which the MAP has an active connection. This is the switch that the MAP used for booting and configuration and is using for data transfer.

See Also

- **display {ap | dap} config** on page 290
- **display dap global** on page 314
- **display dap unconfigured** on page 316

display dap global

Displays connection information for Distributed MAPs configured on a WX switch.

Syntax — **display dap global** [*dap-num* | **serial-id** *serial-ID*]

- *dap-num* — Number of a Distributed MAP for which to display configuration settings.
- **serial-id** *serial-ID* — MAP access point serial ID.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — Connections are shown only for the Distributed MAPs that are configured on the WX switch from which you enter the command, and only for the Mobility Domain the switch is in.

To show information only for Distributed MAPs that have active connections, use the **display dap connection** command.

Examples — The following command displays configuration information for all the Distributed MAPs configured on a WX switch:

```
WX4400# display dap global
Total number of entries: 8
DAP Serial Id     WX IP Address   Bias
--- -----------   --------------- ----
1   M9DE48B012F00 10.3.8.111      HIGH
-   M9DE48B012F00 10.4.3.2        LOW
2   M9DE48B123400 10.3.8.111      LOW
-   M9DE48B123400 10.4.3.2        HIGH
17  M9DE48B123600 10.3.8.111      HIGH
-   M9DE48B123600 10.4.3.2        LOW
18  M9DE48B123700 10.3.8.111      LOW
-   M9DE48B123700 10.4.3.2        HIGH
```

Table 61 describes the fields in this display.

Table 61 Output for display dap global

Field	Description
DAP	Connection ID you assigned to the Distributed MAP. **Note:** DAP numbers are listed only for Distributed MAPs configured on this WX switch. If the field contains a hyphen (**-**), the Distributed MAP configuration displayed in the row of output is on another WX switch.
Serial Id	Serial ID of the Distributed MAP.
WX IP Address	System IP address of the WX switch on which the Distributed MAP is configured. A separate row of output is displayed for each WX switch on which the Distributed MAP is configured.
Bias	Bias of the WX switch for the Distributed MAP: ▪ High ▪ Low

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display {ap | dap} config** on page 290
- **display dap connection** on page 313
- **display dap unconfigured** on page 316
- **set dap** on page 81
- **set {ap | dap} bias** on page 328

display dap unconfigured

Displays Distributed MAPs that are physically connected to the network but that are not configured on any WX switches.

Syntax — **`display dap unconfigured`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command also displays a MAP that is directly connected to a WX switch, if the WX port to which the MAP is connected is configured as a network port instead of a MAP access port, and if the network port is a member of a VLAN.

If a Distributed MAP is configured on a WX switch in another Mobility Domain, the MAP can appear in the output until the MAP is able to establish a connection with a WX switch in its Mobility Domain. After the MAP establishes a connection, the entry for the MAP ages out and no longer appears in the command's output.

Entries in the command output's table age out after two minutes.

Examples — The following command displays information for two Distributed MAPs that are not configured:

```
WX1200# display dap unconfigured
Total number of entries: 2
Serial Id     Model  IP Address      Port Vlan
------------- ------ --------------- ---- --------
M9DE48B012F00 AP2750 10.3.8.54       5    default
M9DE48B123400 AP2750 10.3.8.57       6    vlan-eng
```

Downloaded from www.Manualslib.com manuals search engine

Table 62 describes the fields in this display.

Table 62 Output for display dap unconfigured

Field	Description
Serial Id	Serial ID of the Distributed MAP.
Model	MAP model number.
IP Address	IP address of the MAP. This is the address that the MAP receives from a DHCP server. The MAP uses this address to send a Find WX message to request configuration information from WX switches. However, the MAP cannot use the address to establish a connection unless the MAP first receives a configuration from a WX switch.
Port	Port number on which this WX switch received the MAP's Find WX message.
VLAN	VLAN on which this WX switch received the MAP's Find WX message.

See Also

- **display dap connection** on page 313
- **display dap global** on page 314

display radio-profile

Displays radio profile information.

Syntax — **`display radio-profile`** {*`name`* | **`?`**}

- *`name`* — Displays information about the named radio profile.
- **`?`** — Displays a list of radio profiles.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Name of the backoff timer field changed from Client Backoff Timer to Power Backoff Timer and new fields added in MSS Version 4.0:

- Countermeasures
- Active-Scan
- WMM enabled

Downloaded from www.Manualslib.com manuals search engine

Usage — MSS contains a *default* radio profile. 3Com recommends that you do not change this profile but instead keep the profile for reference.

Examples — The following command shows radio profile information for the *default* radio profile:

```
WX4400# display radio-profile default
Beacon Interval:            100   DTIM Interval:                    1
Max Tx Lifetime:           2000   Max Rx Lifetime:               2000
RTS Threshold:             2346   Frag Threshold:                2346
Short Retry Limit:            5   Long Retry Limit:                 5
Long Preamble:               NO   Allow 802.11g clients only:      NO
Tune Channel:                no   Tune Power:                       no
Tune Channel Interval:     3600   Tune Power Interval:            600
Channel Holddown:           300   Power Backoff Timer:             10
Countmeasures:             none   Active-Scan                    yes
WMM enabled:               yes
Service profiles: default-dot1x, default-clear
```

Table 63 describes the fields in this display.

Table 63 Output for display radio-profile

Field	Description
Beacon Interval	Rate (in milliseconds) at which each MAP radio in the profile advertises the beaconed SSID.
DTIM Interval	Number of times after every beacon that each MAP radio in the radio profile sends a delivery traffic indication map (DTIM).
Max Tx Lifetime	Number of milliseconds that a frame *received* by a radio in the radio profile can remain in buffer memory.
Max Rx Lifetime	Number of milliseconds that a frame *scheduled to be transmitted* by a radio in the radio profile can remain in buffer memory.
RTS Threshold	Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.
Frag Threshold	Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile.
Short Retry Limit	Number of times a radio in the radio profile can send a short unicast frame without receiving an acknowledgment.

Downloaded from www.Manualslib.com manuals search engine

Table 63 Output for display radio-profile (continued)

Field	Description
Long Retry Limit	Number of times a radio in the radio profile can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is *equal to or longer than* the RTS threshold.
Long Preamble	Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only: ■ **YES** — Advertises support for long preambles only. ■ **NO** — Advertises support for long and short preambles.
Allow 802.11g clients only	Indicates whether the 802.11b/g radios in the radio profile restrict associations to 802.11g clients only: ■ **No** — 802.11b/g radios allow associations with both 802.11b and 802.11g clients. ■ **No** — 802.11b/g radios allow associations with 802.11g clients only. **Note:** This field applies only to 802.11b/g radios.
Tune Channel	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels.
Tune Power	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels.
Tune Channel Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.
Tune Power Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.
Power Backoff Timer	Interval, in minutes, at which radios in a radio profile reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting.
Channel Holddown	Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel.

Downloaded from www.Manualslib.com manuals search engine

Table 63 Output for display radio-profile (continued)

Field	Description
Service profiles	Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID. **Note:** When you upgrade from 2.x, MSS creates a default-dot1x service profile for encrypted SSIDs and a default-clear service profile for unencrypted SSIDs. These default service profiles contain the default encryption settings for crypto SSIDs and clear SSIDs, respectively.

See Also

- **set radio-profile 11g-only** on page 347
- **set radio-profile auto-tune channel-config** on page 349
- **set radio-profile auto-tune channel-holddown** on page 350
- **set radio-profile auto-tune channel-interval** on page 351
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354
- **set radio-profile beacon-interval** on page 355
- **set radio-profile dtim-interval** on page 357
- **set radio-profile frag-threshold** on page 358
- **set radio-profile long-retry** on page 359
- **set radio-profile max-rx-lifetime** on page 360
- **set radio-profile max-tx-lifetime** on page 361
- **set radio-profile mode** on page 362
- **set radio-profile preamble-length** on page 364
- **set radio-profile rts-threshold** on page 365
- **set radio-profile service-profile** on page 366
- **set radio-profile short-retry** on page 369

Downloaded from www.Manualslib.com manuals search engine

display service-profile

Displays service profile information.

Syntax — **`display service-profile`** {*`name`* | **`?`**}

- *`name`* — Displays information about the named service profile.
- **`?`** — Displays a list of service profiles.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. New fields added to indicate the configured SSID default attributes in the service profile.

Examples — The following command displays information for service profile *wpa_clients*:

```
WX4400# display service-profile wpa_clients
ssid-name:         private    ssid-type:           crypto
beacon:                yes    auth-fallthru:     web-auth
WEP Key 1 value:     <none>    WEP Key 2 value:     <none>
WEP Key 3 value:     <none>    WEP Key 4 value:     <none>
WEP Unicast Index:        1    WEP Multicast Index:      1
Shared Key Auth:         NO
WPA enabled:
    ciphers: cipher-tkip
    authentication: 802.1X
    TKIP countermeasures time: 60000ms
vlan-name=orange
session-timeout=300
service-type=2
```

Table 64 describes the fields in this display.

Table 64 Output for display service-profile

Field	Description
ssid-name	Service set identifier (SSID) managed by this service profile.
ssid-type	SSID type: ▪ **crypto** — Wireless traffic for the SSID is encrypted. ▪ **clear** — Wireless traffic for the SSID is unencrypted.

Downloaded from www.Manualslib.com manuals search engine

Table 64 Output for display service-profile (continued)

Field	Description
beacon	Indicates whether the radio sends beacons, to advertise the SSID: ▪ no ▪ yes
auth-fallthru	Secondary (fallthru) encryption type when a user tries to authenticate but the WX switch managing the radio does not have an authentication rule with a userglob that matches the username. ▪ **last-resort** — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. ▪ **none**—Denies authentication and prohibits the user from accessing the SSID. ▪ **web-auth** — Redirects the user to a web page for login to the SSID.
WEP Key 1 value	State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP): ▪ **none** —T he key is not configured. ▪ **preset** — The key is configured. **Note:** The WEP parameters apply to traffic only on the encrypted SSID.
WEP Key 2 value	State of static WEP key number 2: ▪ **none** — The key is not configured. ▪ **preset** — The key is configured.
WEP Key 3 value	State of static WEP key number 3: ▪ **none** — The key is not configured. ▪ **preset** — The key is configured.
WEP Key 4 value	State of static WEP key number 4: ▪ **none** — The key is not configured. ▪ **preset** — The key is configured.
WEP Unicast Index	Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.
WEP Multicast Index	Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.
Shared Key Auth	Indicates whether shared-key authentication is enabled.

Downloaded from www.Manualslib.com manuals search engine

Table 64 Output for display service-profile (continued)

Field	Description
WPA enabled	Indicates that the Wi-Fi Protected Access (WPA) information element (IE) is enabled. Additional fields display the settings of other WPA parameters: ▪ **ciphers** — Lists the WPA cipher suites advertised by radios in the radio profile mapped to this service profile. ▪ **authentication** — Lists the authentication methods supported for WPA clients: **802.1X** — dynamic authentication **PSK** — preshared key authentication ▪ **TKIP countermeasures time** — Indicates the amount of time (in ms) MSS enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period. **Note:** The WPA fields are displayed only when the WPA IE is enabled.
vlan-name, session-timeout, service-type	Authorization attributes that are applied by default to a user accessing the SSID managed by this service profile (in addition to any attributes assigned to the user by a RADIUS server or the local database). See Table 44 on page 249 for a list of authorization attributes and values that can be assigned to network users.

See Also

- **set service-profile auth-dot1x** on page 373
- **set service-profile auth-fallthru** on page 374
- **set service-profile auth-psk** on page 375
- **set service-profile beacon** on page 376
- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep104** on page 379
- **set service-profile cipher-wep40** on page 380
- **set service-profile psk-phrase** on page 381
- **set service-profile psk-raw** on page 382
- **set service-profile rsn-ie** on page 383
- **set service-profile shared-key-auth** on page 384

Downloaded from www.Manualslib.com manuals search engine

- **set service-profile ssid-name** on page 384
- **set service-profile ssid-type** on page 385
- **set service-profile tkip-mc-time** on page 386
- **set service-profile web-portal-form** on page 387
- **set service-profile wep active-multicast- index** on page 388
- **set service-profile wep active-unicast- index** on page 389
- **set service-profile wep key-index** on page 390
- **set service-profile wpa-ie** on page 391

reset {ap | dap}

Restarts a MAP access point.

Syntax — **reset** {**ap** *port-list* | **dap** *dap-num*}

- **ap** *port-list* — List of ports connected to the MAP access points to restart.
- **dap** *dap-num* — Number of a Distributed MAP to reset.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — When you enter this command, the MAP access point drops all sessions and reboots.

CAUTION: *Restarting a MAP access point can cause data loss for users who are currently associated with the MAP.*

Examples — The following command resets the MAP access point on port 6:

```
WX1200# reset ap 6
This will reset specified AP devices.
Would you like to continue? (y/n)y
success: rebooting ap attached to port 6
```

Downloaded from www.Manualslib.com manuals search engine

set dap auto

Creates a profile for automatic configuration of Distributed MAPs.

Syntax — **`set dap auto`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Usage — Table 65 lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed MAPs, you must enable the profile using the **set dap auto mode enable** command.

The profile uses the *default* radio profile by default. You can change the profile using the **set dap auto radio radio-profile** command. You can use set dap auto commands to change settings for the parameters listed in Table 65. (The commands are listed in the "See Also" section.)

Table 65 Configurable Profile Parameters for Distributed MAPs

Parameter	Default Value
MAP Parameters	
mode	**disabled**
bias	**high**
upgrade-firmware (boot-download-enable)	**enable** (YES)
group (load balancing group)	none
blink (Not shown in **display dap config** output)	**disable**
Radio Parameters	
radiotype (type)	**11g** (or **11b** for country codes where 802.11g is not allowed)
mode	**enabled**

Downloaded from www.Manualslib.com manuals search engine

Table 65 Configurable Profile Parameters for Distributed MAPs (continued)

Parameter	Default Value
tx-pwr	Highest setting allowed for the country of operation
radio-profile (profile)	**default**
max-power	**default**
min-client-rate	**5.5** for 802.11b/g **24** for 802.11a
max-retransmissions	**10**

Examples — The following command creates a profile for automatic Distributed MAP configuration:

```
WX1200# set dap auto
success: change accepted.
```

See Also

- **set dap auto mode** on page 327
- **set dap auto radiotype** on page 326
- **set {ap | dap} bias** on page 328
- **set {ap | dap} blink** on page 330
- **set {ap | dap} group** on page 332
- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set {ap | dap} radio auto-tune min-client-rate** on page 340
- **set {ap | dap} radio mode** on page 341
- **set {ap | dap} radio radio-profile** on page 343
- **set {ap | dap} upgrade-firmware** on page 346

set dap auto radiotype

Sets the radio type for single-MAP radios that use the MAP configuration profile.

Syntax — **`set dap auto [radiotype {11a | 11b| 11g}]`**

- **`radiotype {11a | 11b| 11g}`** — Radio type. (The 11a option applies only to single-radio models. The 802.11a radio in two-radio models is always 802.11a.):

Downloaded from www.Manualslib.com manuals search engine

- 11a — 802.11a
- 11b — 802.11b
- 11g — 802.11g

Defaults — The default radio type for models AP2750, MP-241, and MP-341, and for the 802.11b/g radios in other models is 802.11g in regulatory domains that support 802.11g, or 802.11b in regulatory domains that do not support 802.11g.

MAP radios configured for 802.11g also allow associations from 802.11b clients by default. To disable support for 802.11b associations, use the **set radio-profile 11g-only** command on the radio profile that contains the radio.

Examples — The following command sets the radio type to 802.11b:

```
WX4400# set dap auto radiotype 11b
success: change accepted.
```

See Also

- **set dap auto** on page 325

set dap auto mode

Enables a WX switch's profile for automatic Distributed MAP configuration.

Syntax — **`set dap auto mode {enable | disable}`**

- **`enable`** — Enables the MAP configuration profile.
- **`disable`** — Disables the MAP configuration profile.

Defaults — The MAP configuration profile is disabled by default.

Access — Enabled.

History —Introduced in MSS 4.0.

Usage — You must use the **set dap auto** command to create the profile before you can enable it.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command enables the profile for automatic Distributed MAP configuration:

```
WX4400# set dap auto mode enable
success: change accepted.
```

See Also

- **set dap auto** on page 325
- **set dap auto radiotype** on page 326
- **set {ap | dap} bias** on page 328
- **set {ap | dap} blink** on page 330
- **set {ap | dap} group** on page 332
- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set {ap | dap} radio auto-tune min-client-rate** on page 340
- **set {ap | dap} radio mode** on page 341
- **set {ap | dap} radio radio-profile** on page 343
- **set {ap | dap} upgrade-firmware** on page 346

set {ap | dap} bias

Changes the bias for a MAP. Bias is the priority of one WX switch over other WX switches for booting and configuring the MAP.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **bias** {**high** | **low**}

- **ap** *port-list* — List of ports on which to change the bias for directly connected MAPs.
- **dap** *dap-num* — Number of a Distributed MAP for which to change the bias.
- **dap auto** — Configures bias for the MAP configuration profile. (See **set dap auto** on page 325.)
- **high** — High bias.
- **low** — Low bias.

Defaults — The default bias is high.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — High bias is preferred over low bias. Bias applies only to WX switches that are indirectly attached to the MAP through an intermediate Layer 2 or Layer 3 network. A MAP always attempts to boot on MAP port 1 first, and if an WX switch is directly attached on MAP port 1, the MAP always boots from it.

If MAP port 1 is indirectly connected to WX switches through the network, the MAP boots from the switch with the high bias for the MAP. If the bias for all connections is the same, the MAP selects the switch that has the greatest capacity to add more active MAPs. For example, if a MAP is dual homed to two WX4400 wireless LAN switches, and one of the switches has 50 active MAPs while the other switch has 60 active MAPs, the new MAP selects the switch that has only 50 active MAPs.

If the boot request on MAP port 1 fails, the MAP attempts to boot over its port 2, using the same process described above.

MAP selection of a WX switch is *sticky*. After a MAP selects a WX switch to boot from, the MAP continues to use that switch for its active data link even if another switch configured with high bias for the MAP becomes available.

Examples — The following command changes the bias for a Distributed MAP to low:

```
WX4400# set dap 1 bias low
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} blink

Enables or disables LED blink mode on a MAP access point to make it easy to identify.

When blink mode is enabled on an AP2750, the 11a LED blinks on and off.

When blink mode is enabled on an AP7250, the Radio LED flashes red and the Power LED flashes green/orange. The Ethernet LED does not change.

When blink mode is enabled on an AP8250, the Radio LED flashes red and the Power LED flashes green/orange. The Ethernet LED does not change.

When blink mode is enabled on an AP8750, both Radio LEDs flash red and the Power LED flashes green/orange. The Ethernet LED does not change.

When blink mode is enabled on other models (MP-*xxx*), the health and radio LEDs alternately blink green and amber. By default, blink mode is disabled.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **blink** {**enable** | **disable**}

- **ap** *port-list* — List of ports connected to the MAP access points on which to turn blink mode on or off.
- **dap** *dap-num* — Number of a Distributed MAP on which to turn blink mode on or off.
- **dap auto** — Configures blink mode for the MAP configuration profile. (See **set dap auto** on page 325.)
- **enable** — Enables blink mode.
- **disable** — Disables blink mode.

Defaults — LED blink mode is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Downloaded from www.Manualslib.com manuals search engine

Usage — Changing the LED blink mode does not alter operation of the MAP access point. Only the behavior of the LEDs is affected.

Examples — The following command enables LED blink mode on the MAP access points connected to ports 3 and 4:

```
WX1200# set ap 3-4 blink enable
success: change accepted.
```

set dap fingerprint

Verifies a MAP's fingerprint on a WX switch. If MAP-WX security is required by a WX switch, a MAP can establish a management session with the switch only if you have verified the MAP's identity by verifying its fingerprint on the switch.

Syntax — **`set dap`** *`num`* **`fingerprint`** *`hex`*

- *`num`* — Number of the Distributed MAP whose fingerprint you are verifying.
- *`hex`* — The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the MAP.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Usage — MAPs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the MAP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If a MAP is already installed and operating, you can use the **display dap status** command to display the fingerprint. The **display dap config** command lists a MAP's fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example verifies the fingerprint for Distributed MAP 8:

```
WX4400# set dap 8 fingerprint
b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

See Also

- **set dap security** on page 345
- **set service-profile cipher-wep40 on page 380** on page 391
- **display {ap | dap} status** on page 304

set {ap | dap} group

Configures a named group of MAP access points. MSS automatically load balances sessions among the access points in a group. To balance the sessions, MSS rejects an association request for an access point's radio if that radio has at least four more active sessions than the radio of the same type with the least number of active sessions within the group.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **group** *name*

- **ap** *port-list* — List of MAP access ports to add to the group.
- **dap** *dap-num* — Number of a Distributed MAP to add to the group.
- **dap auto** — Configures a MAP group for the MAP configuration profile. (See **set dap auto** on page 325.)
- *name* — MAP access point group name of up to 16 alphanumeric characters, with no spaces.

Defaults — MAP access points are not grouped by default.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — You can assign any subset or all of the MAP access points connected to an WX switch to a group on that switch. All access points in a group must be connected to the same WX switch.

Downloaded from www.Manualslib.com manuals search engine

If you use the name *none*, spelled in any combination of capital or lowercase letters, the specified MAP access point is cleared from all MAP access point groups.

Examples — The following command configures a MAP access point group named *loadbalance1* that contains the MAP access points on ports 1, 3, and 5:

```
WX1200# set ap 1,3,5 group loadbalance1
success: change accepted.
```

The following command removes the MAP access point on port 4 from all MAP access point groups:

```
WX1200# set ap 4 group none
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290
- **display {ap | dap} group** on page 303

set {ap | dap} name

Changes a MAP name.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num*} **name** *name*

- **ap** *port-list* — List of ports connected to the MAP access point to rename.
- **dap** *dap-num* — Number of a Distributed MAP to rename.
- *name* — Alphanumeric string of up to 16 characters, with no spaces.

Defaults — The default name of a directly attached MAP is based on the port number of the MAP access port attached to the MAP. For example, the default name for a MAP on MAP access port 1 is *MAP01*. The default name of a Distributed MAP is based on the number you assign to it when you configure the connection. For example, the default name for Distributed MAP 1 is *DAP01*.

Access — Enabled.

History —Introduced in MSS Version 3.0. Default Distributed MAP name changed from DMP*num* to DAP*num* in MSS Version 4.1.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command changes the name of the MAP access point on port 1 to *techpubs*:

```
WX1200# set ap 1 name techpubs
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290

set {ap | dap} radio antennatype

Sets the model number for an external antenna.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num*} **radio** {**1|2**} **antennatype** **{ANT1060** | **ANT1120** | **ANT1180** | **ANT5060** | **ANT5120** | **ANT5180** | **ANT-1360-OUT | ANT-5360-OUT |ANT-5120-OUT | internal**}

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the channel.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the channel.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **antennatype** {**ANT1060** | **ANT1120** | **ANT1180 | internal**} — 802.11b/g external antenna models:
  - **ANT1060** — 60° 802.11b/g antenna
  - **ANT1120** — 120° 802.11b/g antenna
  - **ANT1180** — 180° 802.11b/g antenna
  - **internal** — uses the internal antenna instead
- **antennatype** {**ANT5060** | **ANT5120** | **ANT5180 | internal**} — 802.11a external antenna models:
  - **ANT5060** — 60° 802.11a antenna
  - **ANT5120** — 120° 802.11a antenna
  - **ANT5180** — 180° 802.11a antenna
  - **internal** — uses the internal antenna instead

Downloaded from www.Manualslib.com manuals search engine

- **antennatype** {**ANT-1360-OUT** | **ANT5360-OUT** | **ANT5060 | ANT5120-OUT | internal**} — 802.11a external antenna models:
  - **ANT1360-OUT** — 360° 802.11b/g antenna
  - **ANT5360-OUT** — 360° 802.11a antenna
  - **ANT5060-OUT** — 60° 802.11a antenna
  - **ANT5120-OUT** — 120° 802.11a antenna
  - **internal** — uses the internal antenna instead

Defaults — All radios use the internal antenna by default, if the MAP model has an internal antenna. The MP-620 802.11b/g radio uses model ANT-1360-OUT by default. The MP-620 802.11a radio uses model ANT-5360-OUT by default. The MP-262 802.11b/g radio uses model ANT1060 by default.)

Access — Enabled.

History — Introduced in MSS Version 3.0. Model numbers added for 802.11a external antennas, and the default changed to internal (except for the MP-262) in MSS Version 3.2. Model numbers added for MP-620 external antennas.

Examples — The following command configures the 802.11b/g radio on Distributed MAP 1 to use antenna model ANT1060:

```
WX4400# set dap 1 radio 1 antennatype ANT1060
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290

set {ap | dap} radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **radio** {**1** | **2**} **auto-tune max-power** *power-level*

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the channel.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the channel.

Downloaded from www.Manualslib.com manuals search engine

- **`dap auto`** — Sets the maximum power for radios configured by the MAP configuration profile. (See **set dap auto** on page 325.)
- **`radio 1`** — Radio 1 of the MAP.
- **`radio 2`** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- *`power-level`* — Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation.

  The *power-level* can be a value from 1 to 20.

Defaults — The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Examples — The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the MAP access point on port 6 to 12 dBm.

```
WX1200# set ap 6 radio 1 auto-tune max-power 12
success: change accepted.
```

See Also

- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} radio auto-tune max-retransmissions

Sets the maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio. A high percentage of retransmissions is a symptom of interference on the channel.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **radio** {**1** | **2**} **auto-tune max-retransmissions** *retransmissions*

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the channel.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the channel.
- **dap auto** — Sets the maximum retransmissions for radios configured by the MAP configuration profile. (See **set dap auto** on page 325.)
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- *retransmissions* — Percentage of packets that can result in retransmissions without resulting in a channel change. You can specify from 1 to 100.

Defaults — The default is 10 percent.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — A retransmission is a packet sent from a client to a MAP radio that the radio receives more than once. This can occur when the client does not receive an 802.11 acknowledgement for a packet sent to the radio.

If the radio receives only a single copy of a packet that is transmitted multiple times by a client, the packet is not counted by the radio as a retransmission. For example, if a packet is corrupted and the radio does not receive it, but the second copy of the packet does reach the radio, the radio does not count the packet as a retransmission since the radio received only one recognizable copy of the packet.

Downloaded from www.Manualslib.com manuals search engine

The interval is 1000 packets. If more than the specified percentage of packets within a group of 1000 packets received by the radio are retransmissions, the radio increases power.

When the percentage of retransmissions exceeds the *max-retransmissions* threshold, the radio does not immediately increase power. Instead, if the data rate at which the radio is sending packets to the client is above the minimum data rate allowed, the radio lowers the data rate by one setting. If the retransmissions still exceed the maximum allowed, the radio continues to lower the data rate, one setting at a time, until either the retransmissions fall within the allowed percentile or the minimum allowed data rate is reached.

If the retransmissions still exceed the threshold after the minimum allowed data rate is reached, the radio increases power by 1 dBm. The radio continues increasing the power in 1 dBm increments until the retransmissions fall below the threshold.

After the retransmissions fall below the threshold, the radio reduces power by 1 dBm. As long as retransmissions remain below the threshold, the radio continues reducing power in 1 dBm increments until it returns to its default power level.

A radio also can increase power, in 1 dBm increments, if a client falls below the minimum allowed data rate. After a radio increases power, all clients must be at the minimum data rate or higher and the maximum retransmissions must be within the allowed percentile, before the radio begins reducing power again.

Examples — The following command changes the max-retransmissions value to 20:

```
WX1200# set ap 6 radio 1 auto-tune max-retransmissions 20
success: change accepted.
```

See Also

- **set {ap | dap} radio auto-tune max-power** on page 335
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} radio channel

Sets a MAP radio's channel.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **channel** *channel-number*

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the channel.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the channel.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **channel** *channel-number* — Channel number. The valid channel numbers depend on the country of operation.

Defaults — The default channel depends on the radio type:

- The default channel number for 802.11b/g is 6.
- The default channel number for 802.11a is the lowest valid channel number for the country of operation.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can configure a radio's transmit power on the same command line. Use the **tx-power** option.

This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.

Examples — The following command configures the channel on the 802.11a radio on the MAP access point connected to port 5:

```
WX1200# set ap 5 radio 1 channel 36
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

```
WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display {ap | dap} config** on page 290
- **set {ap | dap} radio tx-power** on page 344

---

set {ap | dap} radio auto-tune min-client-rate

Sets the minimum rate at which a radio is allowed to transmit traffic to clients. The radio automatically increases its transmit power when necessary to maintain at least the minimum rate with an associated client.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **radio** {**1** | **2**} **auto-tune min-client-rate** *rate*

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the channel.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the channel.
- **dap auto** — Sets the radio mode for MAPs managed by the MAP configuration profile. (See **set dap auto** on page 325.)
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- *rate* — Minimum data rate, in megabits per second (Mbps). The valid values depend on the radio type:
  - For 802.11g radios—**54**, **48**, **36**, **24**, **18, 12**, **11**, **9**, **6**, **5.5**, **2**, or **1**
  - For 802.11b radios—**11**, **5.5**, **2**, or **1**
  - For 802.11a radios—**54**, **48**, **36**, **24**, **18**, **12**, **9**, or **6**

Defaults — The default minimum data transmit rate depends on the radio type:

- The default minimum data rate for 802.11b/g and 802.11b radios is 5.5 Mbps.
- The default minimum data rate for 802.11a radios is 24 Mbps.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Downloaded from www.Manualslib.com manuals search engine

Usage — If the data rate for traffic sent by a radio to an associated client falls below the default minimum rate, the radio increases power, in 1 dBm increments, until all clients are at or above the minimum rate.

After all clients are at or above the minimum data transmit rate, the radio reduces power by 1 dBm. As long as the radio continues to transmit at the minimum data rate or higher for all clients, the radio continues reducing power in 1 dBm increments until it returns to its normal power level.

A radio also can increase power, in 1 dBm increments, if more than the allowed percentage of packets received by the radio from a client are retransmissions. After a radio increases power, all clients must be at the minimum data rate or higher and the maximum retransmissions must be within the allowed percentile, before the radio begins reducing power again.

Examples — The following command increases the minimum data rate on radio 1, which is an 802.11b/g radio on the MAP access port on port 6, to 11 Mbps.

```
WX1200# set ap 6 radio 1 min-client-rate 11
success: change accepted.
```

See Also

- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353

set {ap | dap} radio mode

Enables or disables a radio on a MAP access point.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **radio** {**1** | **2**} **mode** {**enable** | **disable**}

- **ap** *port-list* — List of ports connected to the MAP access point(s) on which to turn a radio on or off.
- **dap** *dap-num* — Number of a Distributed MAP on which to turn a radio on or off.
- **dap auto** — Sets the radio mode for MAPs managed by the MAP configuration profile. (See **set dap auto** on page 325.)
- **radio 1** — Radio 1 of the MAP.

Downloaded from www.Manualslib.com manuals search engine

- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **mode enable** — Enables a radio.
- **mode disable** — Disables a radio.

Defaults — MAP access point radios are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — To enable or disable one or more radios to which a profile is assigned, use the **set ap radio radio-profile** command. To enable or disable all radios that use a specific radio profile, use the **set radio-profile** command.

Examples — The following command enables radio 1 on the MAP access points connected to ports 1 through 5:

```
WX1200# set ap 1-5 radio 1 mode enable
success: change accepted.
```

The following command enables radio 2 on ports 1 through 3:

```
WX1200# set ap 1-3 radio 2 mode enable
success: change accepted.
```

See Also

- **clear {ap | dap} radio** on page 286
- **display {ap | dap} config** on page 290
- **set {ap | dap} radio radio-profile** on page 343
- **set radio-profile mode** on page 362

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} radio radio-profile

Assigns a radio profile to a MAP radio and enables or disables the radio.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **radio** {**1** | **2**} **radio-profile** *name* **mode** {**enable** | **disable**}

- **ap** *port-list* — List of ports.
- **dap** *dap-num* — Number of a Distributed MAP.
- **dap auto** — Sets the radio profile for the MAP configuration profile. (See **set dap auto** on page 325.)
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **radio-profile** *name* — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- **mode enable** — Enables radios on the specified ports with the parameter settings in the specified radio profile.
- **mode disable** — Disables radios on the specified ports.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — When you create a new profile, the radio parameters in the profile are set to their factory default values.

To enable or disable all radios that use a specific radio profile, use **set radio-profile**.

Examples — The following command enables radio 1 on ports 3 through 6 assigned to radio profile *rp1*:

```
WX1200# set ap 3-6 radio 1 radio-profile rp1 mode enable
success: change accepted.
```

See Also

- **clear {ap | dap} radio** on page 286
- **display radio-profile** on page 317

Downloaded from www.Manualslib.com manuals search engine

- **set {ap | dap} radio mode** on page 341
- **set radio-profile mode** on page 362

set {ap | dap} radio tx-power

Sets a MAP radio's transmit power.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **tx-power** *power-level*

- **ap** *port-list* — List of ports connected to the MAP access points on which to set the transmit power.
- **dap** *dap-num* — Number of a Distributed MAP on which to set the transmit power.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **tx-power** *power-level* — Number of decibels in relation to 1 milliwatt (dBm). The valid values depend on the country of operation.

  The maximum transmit power you can configure on any 3Com radio is the maximum allowed for the country in which you plan to operate the radio *or* one of the following values if that value is less than the country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g.

Defaults — The default transmit power on all MAP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You also can configure a radio's channel on the same command line. Use the **channel** option.

This command is not valid if dynamic power tuning (RF Auto-Tuning) is enabled.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures the transmit power on the 802.11a radio on the MAP access point connected to port 5:

```
WX1200# set ap 5 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

```
WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290
- **set {ap | dap} radio channel** on page 339

set dap security

Sets security requirements for management sessions between a WX switch and its Distributed MAPs.

This feature applies to Distributed MAPs only, not to directly connected MAPs configured on MAP access ports.

The maximum transmission unit (MTU) for encrypted MAP management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the WX switch and Distributed MAP can support the higher MTU.

Syntax — **`set dap security {require | optional | none}`**

- **`require`** — Requires all Distributed MAPs to have encryption keys that have been verified in the CLI by an administrator. If a MAP does not have an encryption key or the key has not been verified, the WX does not establish a management session with the MAP.
- **`optional`** — Allows MAPs to be managed by the switch even if they do not have encryption keys or their keys have not been verified by an administrator. Encryption is used for MAPs that support it.
- **`none`** — Encryption is not used, even for MAPs that support it.

Defaults — The default setting is **optional**.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS 4.0.

Usage — This parameter applies to all Distributed MAPs managed by the switch. If you change the setting to **required**, the switch requires Distributed MAPs to have encryption keys. The switch also requires their fingerprints to be verified in MSS. When MAP security is required, a MAP can establish a management session with the WX only if its fingerprint has been verified by you in MSS.

A change to MAP security support does not affect management sessions that are already established. To apply the new setting to a MAP, restart the MAP.

Examples — The following command configures a WX to require Distributed MAPs to have encryption keys:

```
WX4400# set dap security require
```

See Also

- **set dap fingerprint** on page 331
- **set service-profile cipher-wep40 on page 380** on page 391
- **display {ap | dap} status** on page 304

set {ap | dap} upgrade-firmware

Disables or reenables automatic upgrade of a MAP access point's boot firmware.

Syntax — **set** {**ap** *port-list* | **dap** *dap-num* | **auto**} **upgrade-firmware** {**enable** | **disable**}

- **ap** *port-list* — List of ports connected to the MAP access point(s) on which to allow automatic firmware upgrades.
- **dap** *dap-num* — Number of a Distributed MAP on which to allow automatic firmware upgrades.
- **dap auto** — Configures firmware upgrades for the MAP configuration profile. (See **set dap auto** on page 325.)
- **enable** — Enables automatic firmware upgrades.
- **disable** — Disables automatic firmware upgrades.

Downloaded from www.Manualslib.com manuals search engine

Defaults — Automatic firmware upgrades of MAP access points are enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Usage — When the feature is enabled on an WX port, a MAP access point connected to that port upgrades its boot firmware to the latest version stored on the WX switch while booting.

Examples — The following command disables automatic firmware upgrades on the MAP access point connected to port 6:

```
WX1200# set ap 6 upgrade-firmware disable
```

See Also

- **display {ap | dap} config** on page 290

---

set radio-profile 11g-only

Configures each 802.11b/g radio in a radio profile to allow associations with 802.11g clients only.

Syntax — **set radio-profile** *name* **11g-only** {**enable** | **disable**}

- *name* — Radio profile name.
- **enable** — Configures radios to allow associations with 802.11g clients only.
- **disable** — Configures radios to allow associations with 802.11g clients and 802.11b clients.

Defaults — The default setting is **disable**. 3Com 802.11b/g radios allow associations with 802.11g and 802.11b clients by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Downloaded from www.Manualslib.com manuals search engine

Even when association of 802.11b clients is disabled, if an 802.11b/g radio detects a beacon from an 802.11b network, the radio enters protection mode to guard against interference.

The **set radio-profile 11g-only** command does not affect the radio support configured with the **set port type ap** command. For example, if you configure a radio to be 802.11b only when you set the port type, the **set radio-profile 11g-only enable** command does not enable 802.11g support on the radio.

Examples — The following command configures the 802.11b/g radios in radio profile *rp1* to allow associations from 802.11g clients only:

```
WX4400# set radio-profile rp1 11g-only enable
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290
- **display radio-profile** on page 317
- **set port type ap** on page 91
- **set radio-profile mode** on page 362

set radio-profile active-scan

Disables or reenables active RF detection scanning on the MAP radios managed by a radio profile. When active scanning is enabled, MAP radios look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

Syntax — **set radio-profile** *name* **active-scan {enable | disable}**

- *name* — Radio profile name.
- **enable** — Configures radios to actively scan for rogues.
- **disable** — Configures radios to scan only passively for rogues by listening for beacons and probe responses.

Downloaded from www.Manualslib.com manuals search engine

Defaults — Active scanning is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The command takes effect only on that switch.

Examples — The following command disables active scan in radio profile *radprof3*:

```
wx4400# set radio-profile radprof3 active-scan disable
success: change accepted.
```

set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

Syntax — **set radio-profile** *name* **auto-tune channel-config** {**enable** | **disable**}

- *name* — Radio profile name.
- **enable** — Configures radios to dynamically select their channels when the radios are started.
- **disable** — Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.

Defaults — Dynamic channel assignment is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you disable RF Auto-Tuning for channels, MSS does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, MSS does not allow you to manually change channels.

Downloaded from www.Manualslib.com manuals search engine

RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64). To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and use the **set {ap | dap} radio channel** command to statically configure the channel.

Examples — The following command disables dynamic channel tuning for radios in the *rp2* radio profile:

```
WX4400# set radio-profile rp2 auto-tune channel-config
disable
success: change accepted.
```

See Also

- **set {ap | dap} radio channel** on page 339
- **set radio-profile auto-tune channel-holddown** on page 350
- **set radio-profile auto-tune channel-interval** on page 351
- **set radio-profile auto-tune power-config** on page 353

set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

Syntax — **set radio-profile** *name* **auto-tune channel-holddown** *holddown*

- *name* — Radio profile name.
- *holddown* — Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

Defaults — The default RF Auto-Tuning channel holddown is 900 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

Examples — The following command changes the channel holddown for radios in radio profile *rp2* to 600 seconds:

```
WX4400# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

See Also

- **set radio-profile auto-tune channel-config** on page 349
- **set radio-profile auto-tune channel-interval** on page 351

set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Syntax — **set radio-profile** *name* **auto-tune channel-interval** *seconds*

- *name* — Radio profile name.
- *seconds* — Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

Defaults — The default channel interval is 3600 seconds (one hour).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — 3Com recommends that you use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio's channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command sets the channel interval for radios in radio profile *rp2* to 2700 seconds (45 minutes):

```
WX4400# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

See Also

- **set radio-profile auto-tune channel-config** on page 349
- **set radio-profile auto-tune channel-holddown** on page 350

set radio-profile auto-tune power-backoff-timer

Sets the interval at which radios in a radio profile reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting.

Syntax — **set radio-profile** *name* **auto-tune power-backoff-timer** *seconds*

- *name* — Radio profile name.
- *seconds* — Number of seconds radios wait before lowering the power by 1 dBm. You can specify from 0 to 65535 seconds.

Defaults — The default power-backoff interval is 10 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

A radio can increase power again if required to preserve the minimum data rate for an associated client.

Examples — The following command changes the power-backoff interval for radios in radio profile *rp2* to 15 seconds:

```
WX4400# set radio-profile rp2 auto-tune
power-backoff-timer 15
success: change accepted.
```

See Also

- **set {ap | dap} radio auto-tune max-power** on page 335

Downloaded from www.Manualslib.com manuals search engine

- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune power-config** on page 353
- **set radio-profile auto-tune power-interval** on page 354

set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

Syntax — **`set radio-profile`** *`name`* **`auto-tune power-config`** {**`enable`** | **`disable`**}

- *`name`* — Radio profile name.
- **`enable`** — Configures radios to dynamically set their power levels when the MAPs are started.
- **`disable`** — Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started.

Defaults — Dynamic power assignment is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.

Examples — The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
WX4400# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

See Also

- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune channel-config** on page 349

Downloaded from www.Manualslib.com manuals search engine

- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-interval** on page 354

set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Syntax — **`set radio-profile`** *`name`* **`auto-tune power-interval`** *`seconds`*

- *`name`* — Radio profile name.
- *`seconds`* — Number of seconds MSS waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds.

Defaults — The default power tuning interval is 300 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — RF Auto-Tuning also can temporarily increase a radio's power level to preserve the minimum data rate for an associated client. In this case, the radio reduces its power in 1 dBm increments until the power returns to the expected level.

Examples — The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
WX4400# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

See Also

- **set {ap | dap} radio auto-tune max-power** on page 335
- **set {ap | dap} radio auto-tune max- retransmissions** on page 337
- **set radio-profile auto-tune power-backoff- timer** on page 352
- **set radio-profile auto-tune power-config** on page 353

Downloaded from www.Manualslib.com manuals search engine

set radio-profile beacon-interval

Changes the rate at which each MAP radio in a radio profile advertises its service set identifier (SSID).

Syntax — **`set radio-profile`** *`name`* **`beacon-interval`** *`interval`*

- *`name`* — Radio profile name.
- *`interval`* — Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults — The beacon interval for MAP radios is 100 ms by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the beacon interval for radio profile *rp1* to 200 ms:

```
WX4400# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362

set radio-profile countermeasures

Enables or disables countermeasures on the MAP radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

CAUTION: *Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.*

Downloaded from www.Manualslib.com manuals search engine

MAP radios can also issue countermeasures against interfering devices. An interfering device is not part of the 3Com network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any WX switch in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with MAP radios.

Syntax — **`set radio-profile`** *`name`* **`countermeasures {all | rogue | configured | none}`**

- *`name`* — Radio profile name.
- **`all`** — Configures radios to attack rogues and interfering devices.
- **`rogue`** — Configures radios to attack rogues only.
- **`configured`** — Configures radios to attack only devices in the attack list on the WX switch (on-demand countermeasures). When this option is specified, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.
- **`none`** — Disables countermeasures for this radio profile.

Defaults — Countermeasures are disabled by default.

Access — Enabled.

History — Command introduced in MSS Version 4.0. New option **configured** added to support on-demand countermeasures in MSS Version 4.1.

Examples — The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
WX1200# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile *radprof3*:

```
WX1200# clear radio-profile radprof3 countermeasures
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

The following command causes radios managed by radio profile *radprof3* to issue countermeasures against devices in the WX switch's attack list:

```
WX1200# set radio-profile radprof3 countermeasures configured
success: change accepted.
```

Note that when you issue this command, countermeasures are then issued only against devices in the WX switch's attack list, not against other devices that were classified as rogues by other means.

set radio-profile dtim-interval

Changes the number of times after every beacon that each MAP radio in a radio profile sends a delivery traffic indication map (DTIM). A MAP access point sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.

The DTIM interval applies to both the beaconed SSID and the nonbeaconed SSID.

Syntax — **set radio-profile** *name* **dtim-interval** *interval*

- *name* — Radio profile name.
- *interval* — Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31.

Defaults — By default, MAP access points send the DTIM once after each beacon.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The DTIM interval does not apply to unicast frames.

Examples — The following command changes the DTIM interval for radio profile *rp1* to 2:

```
WX4400# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362

---

set radio-profile frag-threshold

Changes the fragmentation threshold for the MAP radios in a radio profile. The fragmentation threshold specifies the maximum length a frame is allowed to be without being broken into multiple frames before transmission.

Syntax — **`set radio-profile`** *`name`* **`frag-threshold`** *`threshold`*

- *`name`* — Radio profile name.
- *`threshold`* — Maximum frame length, in bytes. You can enter a value from 256 through 2346.

Defaults — The default fragmentation threshold for MAP radios is 2346 bytes.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the fragmentation threshold for radio profile *rp1* to 1500 bytes:

```
WX4400# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362

Downloaded from www.Manualslib.com manuals search engine

set radio-profile long-retry

Changes the long retry threshold for the MAP radios in a radio profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is *equal to or longer than* the Request-to-Send (RTS) threshold.

Syntax — **`set radio-profile`** *`name`* **`long-retry`** *`threshold`*

- *`name`* — Radio profile name.
- *`threshold`* — Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

Defaults — The default long unicast retry threshold for MAP radios is 5 attempts.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the long retry threshold for radio profile *rp1* to 8:

```
WX4400# set radio-profile rp1 long-retry 8
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362
- **set radio-profile short-retry** on page 369

Downloaded from www.Manualslib.com manuals search engine

set radio-profile max-rx-lifetime

Changes the maximum receive threshold for the MAP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame *received* by a radio can remain in buffer memory.

Syntax — **set radio-profile** *name* **max-rx-lifetime** *time*

- *name* — Radio profile name.
- *time* — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults — The default maximum receive threshold for MAP radios is 2000 ms (2 seconds).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the maximum receive threshold for radio profile *rp1* to 4000 ms:

```
WX4400# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

See Also

- **set radio-profile mode** on page 362
- **set radio-profile max-tx-lifetime** on page 361
- **display radio-profile** on page 317

Downloaded from www.Manualslib.com manuals search engine

set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the MAP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame *scheduled to be transmitted* by a radio can remain in buffer memory.

Syntax — **`set radio-profile`** *`name`* **`max-tx-lifetime`** *`time`*

- *`name`* — Radio profile name.
- *`time`* — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults — The default maximum transmit threshold for MAP radios is 2000 ms (2 seconds).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the maximum transmit threshold for radio profile *rp1* to 4000 ms:

```
WX4400# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362
- **set radio-profile max-rx-lifetime** on page 360

Downloaded from www.Manualslib.com manuals search engine

set radio-profile mode

Creates a new radio profile, or disables or reenables all MAP radios that are using a specific profile.

Syntax — **`set radio-profile`** *`name`* [**`mode`** {**`enable`** | **`disable`**}]

- **`radio-profile`** *`name`* — Radio profile name of up to 16 alphanumeric characters, with no spaces.

  Use this command without the mode enable or **mode disable** option to create a new profile.

- **`mode enable`** — Enables the radios that use this profile.
- **`mode disable`** — Disables the radios that use this profile.

Defaults — Each radio profile that you create has a set of properties with factory default values that you can change with the other **set radio-profile** commands in this chapter. Table 66 lists the parameters controlled by a radio profile and their default values.

Table 66 Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
11g-only	disable	Allows associations with 802.11g and 802.11b clients. **Note:** This parameter applies only to 802.11b/g radios.
active-scan	enable	Sends *probe any* requests (probe requests with a null SSID name) to solicit probe responses from other access points.
auto-tune	enable	Allows dynamic configuration of channel and power settings by MSS.
beacon-interval	100	Waits 100 ms between beacons.
countermeasures	Not configured	Does not issue countermeasures against any device.
dtim-interval	1	Sends the delivery traffic indication map (DTIM) after every beacon.
frag-threshold	2346	Transmits frames up to 2346 bytes long without fragmentation.
long-retry	5	Sends a long unicast frame up to five times without acknowledgment.

Downloaded from www.Manualslib.com manuals search engine

Table 66 Defaults for Radio Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
max-rx-lifetime	2000	Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).
max-tx-lifetime	2000	Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).
preamble-length	short	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. **Note:** This parameter applies only to 802.11b/g radios.
rts-threshold	2346	Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	Default settings for all service profile parameters, including encryption parameters, are used.
short-retry	5	Sends a short unicast frame up to five times without acknowledgment.
wmm	enable	Prioritizes traffic based on the Wi-Fi Multimedia (WMM) standard.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures a new radio profile named *rp1*:

```
WX4400# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile *rp1*:

```
WX4400# set radio-profile rp1 mode enable
```

The following commands disable the radios that use radio profile *rp1*, change the beacon interval, then reenable the radios:

```
WX4400# set radio-profile rp1 mode disable
WX4400# set radio-profile rp1 beacon-interval 200
WX4400# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on MAP radios in radio profile *rp2*:

```
WX4400# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

See Also

- **display {ap | dap} config** on page 290
- **display radio-profile** on page 317
- **set {ap | dap} radio mode** on page 341
- **set {ap | dap} radio radio-profile** on page 343

set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g MAP radio advertises support. This command does not apply to 802.11a.

Syntax — **set radio-profile** *name* *preamble-length* {**long** | **short**}

- *name* — Radio profile name.
- **long** — Advertises support for long preambles.
- **short** — Advertises support for short preambles.

Defaults — The default is **short**.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the MAP access point still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command configures 802.11b/g radios that use the radio profile *rp_long to* advertise support for long preambles instead of short preambles:

```
WX4400# set radio-profile rp_long preamble-length long
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362

set radio-profile rts-threshold

Changes the RTS threshold for the MAP radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

Syntax — **set radio-profile** *name* **rts-threshold** *threshold*

- *name* — Radio profile name.
- *threshold* — Maximum frame length, in bytes. You can enter a value from 256 through 3000.

Defaults — The default RTS threshold for a MAP radio is 2346 bytes.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the RTS threshold for radio profile *rp1* to 1500 bytes:

```
WX4400# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

See Also

- **set radio-profile mode** on page 362
- **display radio-profile** on page 317

set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

Syntax — **set radio-profile** *name* **service-profile** *name*

- **radio-profile** *name* — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- **service-profile** *name* — Service profile name of up to 16 alphanumeric characters, with no spaces.

Defaults — A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. Table 67 lists the parameters controlled by a service profile and their default values.

Table 67 Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
auth-dot1x	enable	When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.

Downloaded from www.Manualslib.com manuals search engine

Table 67 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
auth-fallthru	web-auth	Uses WebAAA for users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.
auth-psk	disable	Does not support using a preshared key (PSK) to authenticate WPA clients.
beacon	enable	Sends beacons to advertise the SSID managed by the service profile.
cipher-ccmp	disable	Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.
cipher-tkip	enable	When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.
cipher-wep104	disable	Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.
cipher-wep40	disable	Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.
psk-phrase	No passphrase defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
psk-raw	No preshared key defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
rsn-ie	disable	Does not use the RSN IE in transmitted frames.
shared-key-auth	disable	Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the **set radio-profile auth-psk** command.
ssid-name	private	Uses the SSID name ***private***.
ssid-type	crypto	Encrypts wireless traffic for the SSID.
tkip-mc-time	60000	Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.

Downloaded from www.Manualslib.com manuals search engine

Table 67 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
web-aaa-form	Not configured	For WebAAA users, serves the default login web page or, if configured, the SSID-specific login web page.
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. If you configure a WEP key for static WEP, MSS continues to also support dynamic WEP.
wep active-multicast-index	1	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	1	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	disable	Does not use the WPA IE in transmitted frames.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command maps service-profile *wpa_clients* to radio profile *rp2*:

```
WX4400# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

See Also

- **display service-profile** on page 321
- **set service-profile auth-dot1x** on page 373
- **set service-profile auth-fallthru** on page 374
- **set service-profile auth-psk** on page 375
- **set service-profile beacon** on page 376

Downloaded from www.Manualslib.com manuals search engine

- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep104** on page 379
- **set service-profile cipher-wep40** on page 380
- **set service-profile psk-phrase** on page 381
- **set service-profile psk-raw** on page 382
- **set service-profile rsn-ie** on page 383
- **set service-profile shared-key-auth** on page 384
- **set service-profile ssid-name** on page 384
- **set service-profile ssid-type** on page 385
- **set service-profile tkip-mc-time** on page 386
- **set service-profile web-portal-form** on page 387
- **set service-profile wep active-multicast- index** on page 388
- **set service-profile wep active-unicast- index** on page 389
- **set service-profile wep key-index** on page 390
- **set service-profile wpa-ie** on page 391

set radio-profile short-retry

Changes the short retry threshold for the MAP radios in a radio profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment.

Syntax — **`set radio-profile`** *`name`* **`short-retry`** *`threshold`*

- *`name`* — Radio profile name.
- *`threshold`* — Number of times the radio can send the same short unicast frame. You can enter a value from 1 through 15.

Defaults — The default short unicast retry threshold for MAP radios is 5 attempts.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the short retry threshold for radio profile *rp1* to 3:

```
WX4400# set radio-profile rp1 short-retry 3
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362
- **set radio-profile long-retry** on page 359

set radio-profile wmm

Disables or reenables Wi-Fi Multimedia (WMM) on the MAP radios in a radio profile.

Syntax — **set radio-profile** *name* **wmm {enable | disable}**

- *name* — Radio profile name.
- **enable** — Enables WMM.
- **disable** — Disables WMM.

Defaults — WMM is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — When WMM is disabled, MAP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the MAP does not tag packets it sends to the WX. Otherwise, classification and tagging remain in effect. (For information, see the "Configuring Quality of Service" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

If you plan to use SpectraLink 802.11 phones, you must enable call admission control (CAC). Use the **set radio-profile wmm admission-control** command.

Downloaded from www.Manualslib.com manuals search engine

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See the "Enabling Prioritization for Legacy Voice over IP" section in the "Configuring and Managing Security ACLs" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

Examples — The following command disables WMM in radio profile *radprofsvp*:

```
WX4400# set radio-profile radprofsvp wmm disable
success: change accepted.
```

See Also

- **set radio-profile mode** on page 362
- **display radio-profile** on page 317

set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

Syntax — **set service-profile** *name* **attr** *attribute-name value*

- *name* — Service profile name.
- *attribute-name value* — Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 44 on page 249. All of the attributes listed in Table 44 can be used with this command except ssid.

Defaults — By default, a service profile does not have any authorization attributes set.

Access — Enabled.

History —Introduced in MSS 4.1.

Usage — To change the value of a default attribute for a service profile, use the set **service-profile attr** command and specify a new value.

Downloaded from www.Manualslib.com manuals search engine

The SSID default attributes are applied *in addition* to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to *2*. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then that user will have a total of two attributes set: **service-type** and **vlan-name**.

If the service profile is configured with the **vlan-name** attribute set to *blue*, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and whether they are set through AAA or through SSID defaults by entering the **display sessions network verbose** command. You can display the configured SSID defaults by entering the **display service-profile** command.

Examples — The following command assigns users accessing the SSID managed by service profile *sp2* to VLAN *blue*:

```
WX4400# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command assigns users accessing the SSID managed by service profile *sp2* to the Mobility Profile *tulip.*

```
WX4400# set service-prof sp2 attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when users accessing the SSID managed by service profile *sp2* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
WX1200# set service-prof sp2 attr time-of-day
Wk1700-0200,Sa,Su
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display service-profile** on page 321
- **display sessions network** on page 525

set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by MAP radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

Syntax — **`set service-profile`**
`name` **`auth-dot1x`** {**`enable`** | **`disable`**}

- *`name`* — Service profile name.
- **`enable`** — Enables 802.1X authentication of WPA clients.
- **`disable`** — Disables 802.1X authentication of WPA clients.

Defaults — When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-dot1x** setting has no effect.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

Examples — The following command disables 802.1X authentication for WPA clients that use service profile *wpa_clients*:

```
WX4400# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display service-profile** on page 321
- **set service-profile auth-psk** on page 375
- **set service-profile psk-phrase** on page 381
- **set service-profile wpa-ie** on page 391

set service-profile auth-fallthru

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user *falls through* to the fallthru method.

The fallthru method is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

Syntax — **`set service-profile`** *`name`* **`auth-fallthru`** {**`last-resort`** | **`none`** | **`web-portal`**}

- **`last-resort`** — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.
- **`none`** — Denies authentication and prohibits the user from accessing the SSID.

  The fallthru authentication type **none** is different from the authentication method **none** you can specify for administrative access. The fallthru authentication type **none** denies access to a network user. In contrast, the authentication method **none** allows access to the WX switch by an administrator. (See "set authentication admin" on page 229 and "set authentication console" on page 231.)
- **`web-portal`** — Serves the user a web page from the WX switch's nonvolatile storage for secure login to the network.

Defaults — The default fallthru authentication type is **web-auth**.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the WX switch that is managing the radio the user is connected to redirects the user to a web page located on the WX switch. The user must type a valid username and password on the web page to access the SSID.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0. Option for WebAAA fallthru authentication type changed from **web-auth** to **web-portal** in MSS Version 4.1.

Usage — The **last-resort** fallthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the **last-resort** method only if none of the SSIDs managed by the service profile require secure access.

The **web-auth** authentication type requires additional configuration items. (See the "Configuring AAA for Network Users" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

Examples — The following command sets the fallthru authentication for SSIDS managed by the service profile *rnd_lab* to none:

```
WX4400# set service-profile rnd_lab auth-fallthru none
success: change accepted.
```

See Also

- **display service-profile** on page 321
- **set web-portal** on page 262
- **set service-profile web-portal-form** on page 387

set service-profile auth-psk

Enables preshared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by MAP radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

Syntax — `set service-profile` *`name`* `auth-psk` {`enable` | `disable`}

- *`name`* — Service profile name.
- **`enable`** — Enables PSK authentication of WPA clients.
- **`disable`** — Disables PSK authentication of WPA clients.

Defaults — When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-psk** setting has no effect.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key. In addition, you must enable the WPA IE.

The WebAAA fallthru authentication type is not supported in conjunction with WPA encryption using preshared keys (PSK) for the same SSID. These options are configurable together but are not compatible. WebAAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place.

Examples — The following command enables PSK authentication for service profile *wpa_clients*:

```
WX4400# set service-profile wpa_clients auth-psk enable
success: change accepted.
```

See Also

- **display service-profile** on page 321
- **set service-profile auth-dot1x** on page 373
- **set service-profile psk-raw** on page 382
- **set service-profile wpa-ie** on page 391

set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service profile.

A MAP radio responds to an 802.11 *probe any* request with only the beaconed SSID(s). For a nonbeaconed SSID, radios respond only to directed 802.11 probe requests that match the nonbeaconed SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

Syntax — **set service-profile** *name* **beacon** {**enable** | **disable**}

- *name* — Service profile name.

Downloaded from www.Manualslib.com manuals search engine

- **enable** — Enables beaconing of the SSID managed by the service profile.
- **disable** — Disables beaconing of the SSID managed by the service profile.

Defaults — Beaconing is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command disables beaconing of the SSID managed by service profile *sp2*:

```
WX4400# set service-profile sp2 beacon disable
success: change accepted.
```

See Also

- **display service-profile** on page 321
- **set radio-profile beacon-interval** on page 355
- **set service-profile ssid-name** on page 384
- **set service-profile ssid-type** on page 385

set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

Syntax — **set service-profile** *name* **cipher-ccmp** {**enable** | **disable**}

- *name* — Service profile name.
- **enable** — Enables CCMP encryption for WPA clients.
- **disable** — Disables CCMP encryption for WPA clients.

Defaults — CCMP encryption is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To use CCMP, you must also enable the WPA IE.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures service profile *sp2* to use CCMP encryption:

```
WX4400# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

See Also

- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep104** on page 379
- **set service-profile cipher-wep40** on page 380
- **set service-profile wpa-ie** on page 391

set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

Syntax — **set service-profile**
name **cipher-tkip** {**enable** | **disable**}

- *name* — Service profile name.
- **enable** — Enables TKIP encryption for WPA clients.
- **disable** — Disables TKIP encryption for WPA clients.

Defaults — When the WPA IE is enabled, TKIP encryption is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To use TKIP, you must also enable the WPA IE.

Examples — The following command disables TKIP encryption in service profile *sp2*:

```
WX4400# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

See Also

- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-wep104** on page 379
- **set service-profile cipher-wep40** on page 380

Downloaded from www.Manualslib.com manuals search engine

- **set service-profile tkip-mc-time** on page 386
- **set service-profile wpa-ie** on page 391

set service-profile cipher-wep104

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

Syntax — **`set service-profile`** *`name`* **`cipher-wep104`** {**`enable`** | **`disable`**}

- *`name`* — Service profile name.
- **`enable`** — Enables 104-bit WEP encryption for WPA clients.
- **`disable`** — Disables 104-bit WEP encryption for WPA clients.

Defaults — 104-bit WEP encryption is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the **set service-profile cipher-wep40** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use 104-bit WEP encryption:

```
WX4400# set service-profile sp2 cipher-wep104 enable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep40** on page 380
- **set service-profile wep key-index** on page 390
- **set service-profile wpa-ie** on page 391

---

set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

Syntax — **`set service-profile`** *`name`* **`cipher-wep40`** {**`enable`** | **`disable`**}

- *`name`* — Service profile name.
- **`enable`** — Enables 40-bit WEP encryption for WPA clients.
- **`disable`** — Disables 40-bit WEP encryption for WPA clients.

Defaults — 40-bit WEP encryption is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures service profile *sp2* to use 40-bit WEP encryption:

```
WX4400# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

See Also

- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep104** on page 379
- **set service-profile wep key-index** on page 390
- **set service-profile wpa-ie** on page 391

set service-profile psk-phrase

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — **set service-profile** *name* **psk-phrase** *passphrase*

- *name* — Service profile name.
- *passphrase* — An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the WX switch's configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures service profile *sp3* to use passphrase "1234567890123<>?=+&% The quick brown fox jumps over the lazy sl":

```
WX4400# set service-profile sp3 psk-phrase "1234567890123<>
?=+&% The quick brown fox jumps over the lazy sl"
success: change accepted.
```

See Also

- **set mac-user attr** on page 249
- **set service-profile auth-psk** on page 375
- **set service-profile psk-raw** on page 382
- **set service-profile wpa-ie** on page 391

set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — **set service-profile** *name* **psk-raw** *hex*

- *name* — Service profile name.
- *hex* — A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults — None.

Examples — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the WX switch's configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures service profile *sp3* to use a raw PSK with PSK clients:

```
WX4400# set service-profile sp3 psk-raw c25d3fe4483e867
d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

See Also

- **set mac-user attr** on page 249
- **set service-profile auth-psk** on page 375
- **set service-profile psk-phrase** on page 381
- **set service-profile wpa-ie** on page 391

set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax — **set service-profile** *name* **rsn-ie** {**enable** | **disable**}

- *name* — Service profile name.
- **enable** — Enables the RSN IE.
- **disable** — Disables the RSN IE.

Defaults — The RSN IE is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command enables the RSN IE in service profile *sprsn*:

```
WX4400# set service-profile sprsn rsn-ie enable
success: change accepted.
```

See Also

- **set service-profile cipher-ccmp** on page 377

Downloaded from www.Manualslib.com manuals search engine

set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.

Use this command only if advised to do so by 3Com. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use the ***set service-profile auth-psk*** *command.*

Syntax — **set service-profile** *name* **shared-key-auth** {**enable** | **disable**}

- *name* — Service profile name.
- **enable** — Enables shared-key authentication.
- **disable** — Disables shared-key authentication.

Defaults — Shared-key authentication is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command enables shared-key authentication in service profile *sp4*:

```
WX4400# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

See Also

- **display radio-profile** on page 317
- **set radio-profile mode** on page 362

set service-profile ssid-name

Configures the SSID name in a service profile.

Syntax — **set service-profile** *name* **ssid-name** *ssid-name*

- *name* — Service profile name.
- *ssid-name* — Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string.

Defaults — The default SSID name is ***private***.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0. Support added for blank spaces in the SSID name in MSS Version 4.0.

Examples — The following command applies the name *guest* to the SSID managed by service profile *clear_wlan*:

```
WX4400# set service-profile clear_wlan ssid-name guest
success: change accepted.
```

See Also

- **set service-profile ssid-type** on page 385

---

set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

Syntax — **set service-profile** *name* **ssid-type** [**clear** | **crypto**]

- *name* — Service profile name.
- **clear** — Wireless traffic for the service profile's SSID is not encrypted.
- **crypto** — Wireless traffic for the service profile's SSID is encrypted.

Defaults — The default SSID type is crypto.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the SSID type for service profile *clear_wlan* to **clear**:

```
WX4400# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

See Also

- **set service-profile ssid-name** on page 384

Downloaded from www.Manualslib.com manuals search engine

set service-profile tkip-mc-time

Changes the length of time that MAP radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, MAP radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

Syntax — **`set service-profile`** *`name`* **`tkip-mc-time`** *`wait-time`*

- *`name`* — Service profile name.
- *`wait-time`* — Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

Defaults — The default countermeasures wait time is 60,000 ms (60 seconds).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

Examples — The following command changes the countermeasures wait time for service profile *sp3* to 30,000 ms (30 seconds):

```
WX4400# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

See Also

- **set service-profile cipher-tkip** on page 378
- **set service-profile wpa-ie** on page 391

Downloaded from www.Manualslib.com manuals search engine

set service-profile web-portal-form

Specifies a custom login page to serve to WebAAA users who request the SSID managed by the service profile.

Syntax — **`set service-profile`** *`name`* **`web-portal-form`** *`url`*

- *`name`* — Service profile name.
- *`url`* — WX subdirectory name and HTML page name of the login page. Specify the full path. For example, *corpa-ssid/corpa.html*.

Defaults — The 3Com Web login page is served by default.

Access — Enabled.

History —Introduced in MSS Version 3.0. Option name changed from **web-aaa-form** to **web-portal-form**, to reflect change to portal-based implementation in MSS Version 4.0.

Usage — 3Com recommends that you create a subdirectory for the custom page and place all the page's files in that subdirectory. Do not place the custom page in the root directory of the switch's user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.

To use WebAAA, the fallthru authentication type in the service profile that manages the SSID must be set to ***web****. To use WebAAA for a wired authentication port, edit the port configuration with the* ***set port type wired-auth*** *command.*

Examples — The following commands create a subdirectory named *corpa-ssid*, copy a custom login page named *corpa-login.html* and a jpg image named *corpa-logo.jpg* into that subdirectory, and set the Web login page for service profile to *corpa-login.html*:

```
WX4400# mkdir corpa-ssid
success: change accepted.
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa-ssid/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
WX4400# copy tftp://10.1.1.1/corpa-logo.jpg corpa-ssid/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]
WX4400# dir corpa-ssid
================================================================================
file:
Filename                                        Size          Created
```

Downloaded from www.Manualslib.com manuals search engine

```
file:corpa-login.html                          637 bytes   Aug 12 2004, 15:42:26
file:corpa-logo.jpg                           1202 bytes   Aug 12 2004, 15:57:11
Total:        1839 bytes used, 206577 Kbytes free
WX4400# set service-profile corpa-service web-aaa-form corpa-ssid/
corpa-login.html
success: change accepted.
```

See Also

- **copy** on page 567
- **dir** on page 570
- **display service-profile** on page 321
- **mkdir** on page 580
- **set port type wired-auth** on page 94
- **set service-profile auth-fallthru** on page 374
- **set web-portal** on page 262

set service-profile wep active-multicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

Syntax — **set service-profile** *name* **wep active-multicast-index** *num*

- *name* — Service profile name.
- *num* — WEP key number. You can enter a value from 1 through 4.

Defaults — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt multicast frames, by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use WEP key 2 for encrypting multicast traffic:

```
WX4400# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set service-profile wep active-unicast- index** on page 389
- **set service-profile wep key-index** on page 390

set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax — **`set service-profile`** *`name`* **`wep active-unicast-index`** *`num`*

- *`name`* — Service profile name.
- *`num`* — WEP key number. You can enter a value from 1 through 4.

Defaults — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt unicast frames, by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use WEP key 4 for encrypting unicast traffic:

```
WX4400# set service-profile sp2 wep active-unicast-index 4
success: change accepted.
```

See Also

- **set service-profile wep active-multicast- index** on page 388
- **set service-profile wep key-index** on page 390

Downloaded from www.Manualslib.com manuals search engine

set service-profile wep key-index

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

Syntax — **set service-profile** *name* **wep key-index** *num* **key** *value*

- *name* — Service profile name.
- **key-index** *num* — WEP key index. You can enter a value from 1 through 4.
- **key** *value* — Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-digit hexadecimal number or a 26-character ASCII string representing a 13-digit hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported:
  - 0 to 9
  - A to F
  - a to f

Defaults — By default, no static WEP keys are defined.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS automatically enables static WEP when you define a WEP key. MSS continues to support dynamic WEP.

If you plan to use static WEP, do not map more than 8 service profiles that contain static WEP keys to the same radio profile.

Examples — The following command configures WEP key index 1 for service profile *sp2* to *aabbccddee*:

```
WX4400# set service-profile sp2 wep key-index 1 key
aabbccddee
success: change accepted.
```

See Also

- **set service-profile wep active-multicast- index** on page 388
- **set service-profile wep active-unicast- index** on page 389

Downloaded from www.Manualslib.com manuals search engine

set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax — **`set service-profile`** *`name`* **`wpa-ie`** {**`enable`** | **`disable`**}

- *`name`* — Service profile name.
- **`enable`** — Enables the WPA IE.
- **`disable`** — Disables the WPA IE.

Defaults — The WPA IE is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples — The following command enables the WPA IE in service profile *sp2*:

```
WX4400# set service-profile sp2 wpa-ie enable
success: change accepted.
```

See Also

- **set service-profile auth-dot1x** on page 373
- **set service-profile auth-psk** on page 375
- **set service-profile cipher-ccmp** on page 377
- **set service-profile cipher-tkip** on page 378
- **set service-profile cipher-wep104** on page 379
- **set service-profile cipher-wep40** on page 380

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

12 STP COMMANDS

Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on a wireless LAN switch or controller, to maintain a loop-free network.

STP Commands by Usage

This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 68 STP Commands by Usage

Type	Command
STP State	**set spantree** on page 410
	display spantree on page 398
	display spantree blockedports on page 401
Bridge Priority	**set spantree priority** on page 419
Port Cost	**set spantree portcost** on page 414
	set spantree portvlancost on page 417
	display spantree portvlancost on page 403
	clear spantree portcost on page 394
	clear spantree portvlancost on page 395
Port Priority	**set spantree portpri** on page 416
	set spantree portvlanpri on page 418
	clear spantree portpri on page 395
	clear spantree portvlanpri on page 396
Timers	**set spantree fwddelay** on page 412
	set spantree hello on page 412
	set spantree maxage on page 413
Fast Convergence	**set spantree portfast** on page 415
	display spantree portfast on page 402

Downloaded from www.Manualslib.com manuals search engine

Table 68 STP Commands by Usage (continued)

Type	Command
Fast Convergence, cont.	**set spantree backbonefast** on page 411
	display spantree backbonefast on page 400
	set spantree uplinkfast on page 419
	display spantree uplinkfast on page 409
Statistics	**display spantree statistics** on page 403
	clear spantree statistics on page 397

clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on a WX switch.

Syntax — **`clear spantree portcost`** *`port-list`*

- *`port-list`* — List of ports. The port cost is reset on the specified ports.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the **clear spantree portvlancost** command.

Examples — The following command resets the STP port cost on ports 5 and 6 to the default value:

```
WX1200# clear spantree portcost 5-6
success: change accepted.
```

See Also

- **clear spantree portvlancost** on page 395
- **display spantree** on page 398
- **display spantree portvlancost** on page 403
- **set spantree portcost** on page 414
- **set spantree portvlancost** on page 417

Downloaded from www.Manualslib.com manuals search engine

clear spantree portpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on a wireless LAN switch or controller.

Syntax — **`clear spantree portpri`** *`port-list`*

- *`port-list`* — List of ports. The port priority is reset to 32 (the default) on the specified ports.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command resets the priority in all VLANs. To reset the priority for only specific VLANs, use the **clear spantree portvlanpri** command.

Examples — The following command resets the STP priority on port 6 to the default:

```
WX1200# clear spantree portpri 6
success: change accepted.
```

See Also

- **clear spantree portvlanpri** on page 396
- **display spantree** on page 398
- **set spantree portpri** on page 416
- **set spantree portvlanpri** on page 418

clear spantree portvlancost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch, or for all VLANs.

Syntax — **`clear spantree portvlancost`** *`port-list`* {**`all`** | **`vlan`** *`vlan-id`*}

- *`port-list`* — List of ports. The port cost is reset on the specified ports.
- **`all`** — Resets the cost for all VLANs.

Downloaded from www.Manualslib.com manuals search engine

- **vlan** *vlan-id* — VLAN name or number. MSS resets the cost for only the specified VLAN.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS does not change a port's cost for VLANs other than the one(s) you specify.

Examples — The following command resets the STP cost for port 2 in VLAN sunflower:

```
WX4400# clear spantree portvlancost 2 vlan sunflower
success: change accepted.
```

See Also

- **clear spantree portcost** on page 394
- **display spantree** on page 398
- **display spantree portvlancost** on page 403
- **set spantree portcost** on page 414
- **set spantree portvlancost** on page 417

clear spantree portvlanpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax — **clear spantree portvlanpri** *port-list* {**all** | **vlan** *vlan-id*}

- *port-list* — List of ports. The port priority is reset to 32 (the default) on the specified ports.
- **all** — Resets the priority for all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS resets the priority for only the specified VLAN.

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

Usage — MSS does not change a port's priority for VLANs other than the one(s) you specify.

Examples — The following command resets the STP priority for port 2 in VLAN avocado:

```
WX4400# clear spantree portvlanpri 2 vlan avocado
success: change accepted.
```

See Also

- **clear spantree portpri** on page 395
- **display spantree** on page 398
- **set spantree portpri** on page 416
- **set spantree portvlanpri** on page 418

clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

Syntax — **clear spantree statistics** *port-list* [**vlan** *vlan-id*]

- *port-list* — List of ports. Statistics counters are reset on the specified ports.
- **vlan** *vlan-id* — VLAN name or number. MSS resets statistics counters for only the specified VLAN.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command clears STP statistics counters for ports 1, 3, and 5 through 8, for all VLANs:

```
WX1200# clear spantree statistics 1,3,5-8
success: change accepted.
```

See Also

- **display spantree statistics** on page 403

Downloaded from www.Manualslib.com manuals search engine

display spantree

Displays STP configuration and port-state information.

Syntax — **display spantree**
[*port-list* | **vlan** *vlan-id*] [**active**]

- *port-list* — List of ports. If you do not specify any ports, MSS displays STP information for all ports.
- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays STP information for all VLANs.
- **active** — Displays information for only the active (forwarding) ports.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays STP information for VLAN default:

```
WX1200# display spantree vlan default
VLAN     1
Spanning tree mode           PVST+
Spanning tree type           IEEE
Spanning tree enabled

Designated Root              00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost    19
Designated Root Port         1
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-02-76-f7
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               Vlan       Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------------
1                   1        Forwarding      19   128     Disabled
2                   1        Disabled        19   128     Disabled
3                   1        Disabled        19   128     Disabled
4                   1        Disabled        19   128     Disabled
5                   1        Disabled        19   128     Disabled
6                   1        Forwarding      19   128     Disabled
7                   1        Disabled        19   128     Disabled
8                   1        Disabled        19   128     Disabled
```

Downloaded from www.Manualslib.com manuals search engine

Table 69 describes the fields in this display.

Table 69 Output for display spantree

Field	Description
VLAN	VLAN number.
Spanning tree mode	In the current software version, the mode is always *PVST+,* which means Per VLAN Spanning Tree+.
Spanning tree type	In the current software version, the type is always *IEEE,* which means MSS STP is 802.1D-compatible.
Spanning tree enabled	State of STP on the VLAN.
Designated Root	MAC address of the spanning tree's root bridge.
Designated Root Priority	Bridge priority of the root bridge.
Designated Root Path Cost	Cumulative cost from this bridge to the root bridge. If this WX switch is the root bridge, then the root cost is 0.
Designated Root Port	Port through which this WX switch reaches the root bridge. If this WX switch is the root bridge, this field says *We are the root.*
Root Max Age	Maximum acceptable age for hello packets on the root bridge.
Root Hello Time	Hello interval on the root bridge.
Root Forward Delay	Forwarding delay value on the root bridge.
Bridge ID MAC ADDR	This WX switch's MAC address.
Bridge ID Priority	This WX switch's bridge priority.
Bridge Max Age	This WX switch's maximum acceptable age for hello packets.
Bridge Hello Time	This WX switch's hello interval.
Bridge Forward Delay	This WX switch's forwarding delay value.
Port	Port number. Only network ports are listed. STP does not apply to 3Com Wireless LAN Managed Access Point AP2750 ports or wired authentication ports.
Vlan	VLAN ID.

Downloaded from www.Manualslib.com manuals search engine

Table 69 Output for display spantree (continued)

Field	Description
Port-State	STP state of the port: ▪ **Blocking** — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ▪ **Disabled** — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. ▪ **Forwarding** — The port is forwarding Layer 2 traffic. ▪ **Learning** — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding. ▪ **Listening** — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.
Cost	STP cost of the port.
Prio	STP priority of the port.
Portfast	State of the uplink fast convergence feature: ▪ Enabled ▪ Disabled

See Also

- **display spantree blockedports** on page 401

display spantree backbonefast

Indicates whether the STP backbone fast convergence feature is enabled or disabled.

Syntax — **`display spantree backbonefast`**

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example shows the command output on a WX switch with backbone fast convergence enabled:

```
WX4400# display spantree backbonefast


 Backbonefast is enabled
```

See Also

- **set spantree backbonefast** on page 411

display spantree blockedports

Lists information about wireless LAN switch ports that STP has blocked on one or all of its VLANs.

Syntax — **display spantree blockedports** [**vlan** *vlan-id*]

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Usage — The command lists information separately for each VLAN.

Examples — The following command shows information about blocked ports on a WX switch for the default VLAN (VLAN 1):

```
WX4400# display spantree blockedports vlan default

Port               Vlan       Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------
2                  190        Blocking         4   128     Disabled

Number of blocked ports (segments) in VLAN 1 : 1
```

The port information is the same as the information displayed by the **display spantree** command. See Table 69 on page 399.

See Also

- **display spantree** on page 398

Downloaded from www.Manualslib.com manuals search engine

display spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

Syntax — **display spantree portfast** [*port-list*]

- *port-list* — List of ports. If you do not specify any ports, MSS displays uplink fast convergence information for all ports.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command shows uplink fast convergence information for all ports:

```
WX1200# display spantree portfast
Port                        Vlan   Portfast
--------------------------- ----   ----------
1                           1      disable
2                           1      disable
3                           1      disable
4                           1      enable
5                           1      disable
6                           1      disable
7                           1      disable
8                           1      disable
```

Table 70 describes the fields in this display.

Table 70 Output for display spantree portfast

Field	Description
Port	Port number.
VLAN	VLAN number.
Portfast	State of the uplink fast convergence feature: ▪ Enable ▪ Disable

See Also

- **set spantree portfast** on page 415

Downloaded from www.Manualslib.com manuals search engine

display spantree portvlancost

Shows the cost of a port on a path to the STP root bridge, for each of the port's VLANs.

Syntax — **`display spantree portvlancost`** *`port-list`*

- *`port-list`* — List of ports.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command shows the STP port cost of port 1:

```
WX4400# display spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

See Also

- **clear spantree portcost** on page 394
- **clear spantree portvlancost** on page 395
- **display spantree** on page 398
- **set spantree portcost** on page 414
- **set spantree portvlancost** on page 417

display spantree statistics

Displays STP statistics for one or more WX network ports.

Syntax — **`display spantree statistics`**
[*`port-list`* [**`vlan`** *`vlan-id`*]]

- *`port-list`* — List of ports. If you do not specify any ports, MSS displays STP statistics for all ports.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — The command displays statistics separately for each port.

Examples — The following command shows STP statistics for port 1:

```
WX4400# display spantree statistics 1

BPDU related parameters


Port 1                    VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree                          enabled
state                                       Forwarding
port_id                                     0x8015
port_number                                 0x5
path cost                                   0x4
message age (port/VLAN)                     0(20)
designated_root                             00-0b-0e-00-04-30
designated cost                             0x0
designated_bridge                           00-0b-0e-00-04-30
designated_port                             38
top_change_ack                              FALSE
config_pending                              FALSE
port_inconsistency                          none


             Port based information statistics

config BPDU's xmitted(port/VLAN)            0 (1)
config BPDU's received(port/VLAN)           21825 (43649)
tcn BPDU's xmitted(port/VLAN)               0 (0)
tcn BPDU's received(port/VLAN)              2 (2)
forward transition count (port/VLAN)        1 (1)
scp failure count                           0
root inc trans count (port/VLAN)            1 (1)
inhibit loopguard                           FALSE
loop inc trans count                        0 (0)


            Status of Port Timers

forward delay timer                         INACTIVE
forward delay timer value                   15
message age timer                           ACTIVE
message age timer value                     0
topology change timer                       INACTIVE
```

Downloaded from www.Manualslib.com manuals search engine

```
topology change timer value              0
hold timer                               INACTIVE
hold timer value                         0
delay root port timer                    INACTIVE
delay root port timer value              0
delay root port timer restarted is       FALSE


             VLAN based information & statistics

spanning tree type                       ieee
spanning tree multicast address          01-00-0c-cc-cc-cd
bridge priority                          32768
bridge MAC address                       00-0b-0e-12-34-56
bridge hello time                        2
bridge forward delay                     15
topology change initiator:               0
last topology change occured:            Tue Jul 01 2003 22:33:36.
topology change                          FALSE
topology change time                     35
topology change detected                 FALSE
topology change count                    1
topology change last recvd. from         00-0b-0e-02-76-f6


             Other port specific info

dynamic max age transition               0
port BPDU ok count                       21825
msg age expiry count                     0
link loading                             0
BPDU in processing                       FALSE
num of similar BPDU's to process         0
received_inferior_bpdu                   FALSE
next state                               0
src MAC count                            21807
total src MAC count                      21825
curr_src_mac                             00-0b-0e-00-04-30
next_src_mac                             00-0b-0e-02-76-f6
```

Table 71 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 71 Output for display spantree statistics

Field	Description
Port	Port number.
VLAN	VLAN ID.
Spanning Tree enabled for vlan	State of the STP feature on the VLAN.
port spanning tree	State of the STP feature on the port.
state	STP state of the port: ▪ **Blocking** — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ▪ **Disabled** — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. ▪ **Forwarding** — The port is forwarding Layer 2 traffic. ▪ **Learning** — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding. ▪ **Listening** — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.
port_id	STP port ID.
port_number	STP port number.
path cost	Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost).
message age	Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch.
designated_root	MAC address of the root bridge.
designated cost	Total path cost to reach the root bridge.
designated_bridge	Bridge to which this switch forwards traffic away from the root bridge.
designated_port	STP port through which this switch forwards traffic away from the root bridge.
top_change_ack	Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU.

Downloaded from www.Manualslib.com manuals search engine

Table 71 Output for display spantree statistics (continued)

Field	Description
config_pending	Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port.
port_inconsistency	Indicates whether the port is in an inconsistent state.
config BPDU's xmitted	Number of BPDUs transmitted from the port. A number in parentheses indicates the number of configured BPDUs transmitted by the WX switch for this VLAN's spanning tree.
config BPDU's received	Number of BPDUs received by this port. A number in parentheses indicates the number of configured BPDUs received by the WX switch for this VLAN's spanning tree.
tcn BPDU's xmitted	Number of topology change notification (TCN) BDPUs transmitted on this port.
tcn BPDU's received	Number of TCN BPDUs received on this port.
forward transition count	Number of times the port state transitioned to the forwarding state.
scp failure count	Number of service control point (SCP) failures.
root inc trans count	Number of times the root bridge changed.
inhibit loopguard	State of the loop guard. In the current release, the state is always FALSE.
loop inc trans count	Number of loops that have occurred.
forward delay timer	Status of the forwarding delay timer. This timer monitors the time spent by a port in the listening and learning states.
forward delay timer value	Current value of the forwarding delay timer, in seconds.
message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer, in seconds.
topology change timer	Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change.
topology change timer value	Current value of the topology change timer, in seconds.

Downloaded from www.Manualslib.com manuals search engine

Table 71 Output for display spantree statistics (continued)

Field	Description
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer, in seconds.
delay root port timer	Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled.
delay root port timer value	Current value of the delay root port timer.
delay root port timer restarted is	Whether the delay root port timer has been restarted.
spanning tree type	Type of spanning tree. The type is always IEEE.
spanning tree multicast address	Destination address used to send out configured BPDUs on a bridge port.
bridge priority	STP priority of this WX switch.
bridge MAC address	MAC address of this WX switch.
bridge hello time	Value of the hello timer interval, in seconds, when this WX switch is the root or is attempting to become the root.
bridge forward delay	Value of the forwarding delay interval, in seconds, when this WX switch is the root or is attempting to become the root.
topology change initiator	Port number that initiated the most recent topology change.
last topology change occurred	System time when the most recent topology change occurred.
topology change	Value of the topology change flag in configuration BPDUs to be transmitted by this WX switch on VLANs for which the switch is the designated bridge.
topology change time	Time period, in seconds, during which BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change. It is equal to the sum of the switch's maximum age and forwarding delay parameters.
topology change detected	Indicates whether a topology change has been detected by the switch.
topology change count	Number of times the topology change has occurred.
topology change last recvd. from	MAC address of the bridge from which the WX switch last received a topology change.

Downloaded from www.Manualslib.com manuals search engine

Table 71 Output for display spantree statistics (continued)

Field	Description
dynamic max age transition	Number of times the maximum age parameter was changed dynamically.
port BPDU ok count	Number of valid port BPDUs received.
msg age expiry count	Number of expired messages.
link loading	Indicates whether the link is oversubscribed.
BPDU in processing	Indicates whether BPDUs are currently being processed.
num of similar BPDU's to process	Number of similar BPDUs received on a port that need to be processed.
received_inferior_bpdu	Indicates whether the port has received an inferior BPDU or a response to a Root Link Query (RLQ) BPDU.
next state	Port state before it is set by STP.
src MAC count	Number of BPDUs with the same source MAC address.
total src MAC count	Number of BPDUs with all the source MAC addresses.
curr_src_mac	Source MAC address of the current received BPDU.
next_src_mac	Other source MAC address from a different source.

See Also

- **clear spantree statistics** on page 397

display spantree uplinkfast

Shows uplink fast convergence information for one VLAN or all VLANs.

Syntax — **`display spantree uplinkfast`** [**`vlan`** *`vlan-id`*]

- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults — None.

Access — All.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows uplink fast convergence information for all VLANs:

```
WX4400# display spantree uplinkfast
 VLAN    port    list
--------------------------------------------------------------------------
1       1(fwd),2,3
```

Table 72 describes the fields in this display.

Table 72 Output for display spantree uplinkfast

Field	Description
VLAN	VLAN number.
port list	Ports in the uplink group. The port that is forwarding traffic is indicated by *fwd*. The other ports are blocking traffic.

See Also

- **set spantree uplinkfast** on page 419

set spantree

Enables or disables STP on one VLAN or all VLANs configured on a WX switch.

Syntax — **set spantree** {**enable** | **disable** } [{**all** | **vlan** *vlan-id* | **port** *port-list vlan-id*}]

- **enable** — Enables STP.
- **disable** — Disables STP.
- **all** — Enables or disables STP on all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS enables or disables STP on only the specified VLAN, on all ports within the VLAN.
- **port** *port-list vlan-id* — Port number or list and the VLAN the ports are in. MSS enables or disables STP on only the specified ports, within the specified VLAN.

Defaults — Disabled.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command enables STP on all VLANs configured on a WX switch:

```
WX4400# set spantree enable
success: change accepted.
```

The following command disables STP on VLAN burgundy:

```
WX4400# set spantree disable vlan burgundy
success: change accepted.
```

See Also

- **display spantree** on page 398

set spantree backbonefast

Enables or disables STP backbone fast convergence on a wireless LAN switch. This feature accelerates a port's recovery following the failure of an indirect link.

CAUTION: *The backbone fast convergence feature is not compatible with switches that are running standard IEEE 802.1D Spanning Tree implementations. This includes switches running Rapid Spanning Tree or Multiple Spanning Tree.*

Syntax — **set spantree backbonefast** {**enable** | **disable**}

- **enable** — Enables backbone fast convergence.
- **disable** — Disables backbone fast convergence.

Defaults — STP backbone fast path convergence is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

Examples — The following command enables backbone fast convergence:

```
WX4400# set spantree backbonefast enable
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display spantree backbonefast** on page 400

---

set spantree fwddelay

Changes the period of time after a topology change that a WX switch which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of its configured VLANs. (The root bridge always forwards traffic.)

Syntax — **set spantree fwddelay delay** {**all** | **vlan** *vlan-id*}

- **delay** — Delay value. You can specify from 4 through 30 seconds.
- **all** — Changes the forwarding delay on all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

Defaults — The default forwarding delay is 15 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the forwarding delay on VLAN *pink* to 20 seconds:

```
WX4400# set spantree fwddelay 20 vlan pink
success: change accepted.
```

See Also

- **display spantree** on page 398

---

set spantree hello

Changes the interval between STP hello messages sent by a wireless LAN switch when operating as the root bridge, on one or all of its configured VLANs.

Syntax — **set spantree hello interval** {**all** | **vlan** *vlan-id*}

- **interval** — Interval value. You can specify from 1 through 10 seconds.
- **all** — Changes the interval on all VLANs.

Downloaded from www.Manualslib.com manuals search engine

- **vlan** *vlan-id* — VLAN name or number. MSS changes the interval on only the specified VLAN.

Defaults — The default hello timer interval is 2 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the hello interval for all VLANs to 4 seconds:

```
WX4400# set spantree hello 4 all
success: change accepted.
```

See Also

- **display spantree** on page 398

set spantree maxage

Changes the maximum age for an STP root bridge hello packet that is acceptable to a wireless LAN switch acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the WX switch determines that the root bridge is unavailable and issues a topology change message.

Syntax — **set spantree maxage** *aging-time* {**all** | **vlan** *vlan-id*}

- *aging-time* — Maximum age value. You can specify from 6 through 40 seconds.
- **all** — Changes the maximum age on all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS changes the maximum age on only the specified VLAN.

Defaults — The default maximum age for root bridge hello packets is 20 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
WX4400# set spantree maxage 15 all
success: change accepted.
```

See Also

- **display spantree** on page 398

set spantree portcost

Changes the cost that transmission through a network port or ports in the default VLAN on a wireless LAN switch adds to the total cost of a path to the STP root bridge.

Syntax — **set spantree portcost** *port-list* **cost** *cost*

- *port-list* — List of ports. MSS applies the cost change to all the specified ports.
- **cost** *cost* — Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.

Defaults — The default port cost depends on the port speed and link type. Table 73 lists the defaults for STP port path cost.

Table 73 SNMP Port Path Cost Defaults

Port Speed	Link Type	Default Port Path Cost
1000 Mbps	Full Duplex Aggregate Link (Port Group)	19
1000 Mbps	Full Duplex	4
100 Mbps	Full Duplex Aggregate Link (Port Group)	19
100 Mbps	Full Duplex	18
100 Mbps	Half Duplex	19
10 Mbps	Full Duplex Aggregate Link (Port Group)	19
10 Mbps	Full Duplex	95
10 Mbps	Half Duplex	100

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To change the cost of a port in another VLAN, use the **set spantree portvlancost** command.

Examples — The following command changes the cost on ports 3 and 4 to 20:

```
WX1200# set spantree portcost 3,4 cost 20
success: change accepted.
```

See Also

- **clear spantree portcost** on page 394
- **clear spantree portvlancost** on page 395
- **display spantree** on page 398
- **display spantree portvlancost** on page 403
- **set spantree portvlancost** on page 417

set spantree portfast

Enables or disables STP port fast convergence on one or more ports on a wireless LAN switch.

Syntax — **set spantree portfast port** *port-list* {**enable** | **disable**}

- **port** *port-list* — List of ports. MSS enables the feature on the specified ports.
- **enable** — Enables port fast convergence.
- **disable** — Disables port fast convergence.

Defaults — STP port fast convergence is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command enables port fast convergence on ports 2, 5, and 7:

```
WX1200# set spantree portfast port 2,4,7 enable
success: change accepted.
```

See Also

- **display spantree portfast** on page 402

set spantree portpri

Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on a wireless LAN switch.

Syntax — **set spantree portpri** *port-list* **priority** *value*

- *port-list* — List of ports. MSS changes the priority on the specified ports.
- **priority** *value* — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).

Defaults — The default STP priority for all network ports is 128.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the **set spantree portvlanpri** command.

Examples — The following command sets the priority of ports 3 and 4 to 48:

```
WX1200# set spantree portpri 3-4 priority 48
success: change accepted.
```

See Also

- **clear spantree portpri** on page 395
- **clear spantree portvlanpri** on page 396
- **display spantree** on page 398
- **set spantree portvlanpri** on page 418

Downloaded from www.Manualslib.com manuals search engine

set spantree portvlancost

Changes the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch.

Syntax — **set spantree portvlancost** *port-list* **cost** *cost* {**all** | **vlan** *vlan-id*}

- *port-list* — List of ports. MSS applies the cost change to all the specified ports.
- **cost** *cost* — Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.
- **all** — Changes the cost on all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS changes the cost on only the specified VLAN.

Defaults — The default port cost depends on the port speed and link type. (See Table 68 on page 393.)

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the cost on ports 3 and 4 to 20 in VLAN *mauve*:

```
WX1200# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.
```

See Also

- **clear spantree portcost** on page 394
- **clear spantree portvlancost** on page 395
- **display spantree** on page 398
- **display spantree portvlancost** on page 403
- **set spantree portcost** on page 414

Downloaded from www.Manualslib.com manuals search engine

set spantree portvlanpri

Changes the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax — **`set spantree portvlanpri`**
`port-list` **`priority`** *`value`* {**`all`** | **`vlan`** *`vlan-id`*}

- *`port-list`* — List of ports. MSS changes the priority on the specified ports.
- **`priority`** *`value`* — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).
- **`all`** — Changes the priority on all VLANs.
- **`vlan`** *`vlan-id`* — VLAN name or number. MSS changes the priority on only the specified VLAN.

Defaults — The default STP priority for all network ports is 128.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command sets the priority of ports 3 and 4 to 48 on VLAN *mauve*:

```
WX1200# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

See Also

- **clear spantree portpri** on page 395
- **clear spantree portvlanpri** on page 396
- **display spantree** on page 398
- **set spantree portpri** on page 416

Downloaded from www.Manualslib.com manuals search engine

set spantree priority

Changes the STP root bridge priority of a wireless LAN switch on one or all of its VLANs.

Syntax — **`set spantree priority`** *`value`* {**`all`** | **`vlan`** `vlan-id`}

- **`priority`** *`value`* — Priority value. You can specify a value from 0 through 65,535. The bridge with the lowest priority value is elected to be the root bridge for the spanning tree.
- **`all`** — Changes the bridge priority on all VLANs.
- **`vlan`** *`vlan-id`* — VLAN name or number. MSS changes the bridge priority on only the specified VLAN.

Defaults — The default root bridge priority for the switch on all VLANs is 32,768.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command sets the bridge priority of VLAN *pink* to 69:

```
WX4400# set spantree priority 69 vlan pink
success: change accepted.
```

See Also

- **display spantree** on page 398

set spantree uplinkfast

Enables or disables STP uplink fast convergence on a wireless LAN switch. This feature enables a WX switch with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

Syntax — set spantree uplinkfast {enable | disable}

- enable — Enables uplink fast convergence.
- disable — Disables uplink fast convergence.

Defaults — Disabled.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0.

Usage — The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on WX switches that are in the network core.

Examples — The following command enables uplink fast convergence:

```
WX4400# set spantree uplinkfast enable
success: change accepted.
```

See Also

- **display spantree uplinkfast** on page 409

Downloaded from www.Manualslib.com manuals search engine

13 IGMP SNOOPING COMMANDS

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a WX.

Commands by usage

This chapter presents IGMP snooping commands alphabetically. Use the Table 74 to locate commands in this chapter based on their use.

Table 74 IGMP Commands by Usage

Type	Command
IGMP Snooping State	**set igmp** on page 433
	display igmp on page 422
Proxy Reporting	**set igmp proxy-report** on page 438
Pseudo-querier	**set igmp querier** on page 441
	display igmp querier on page 427
Timers	**set igmp qi** on page 439
	set igmp oqi on page 437
	set igmp qri on page 440
	set igmp lmqi on page 434
	set igmp rv on page 442
Router Solicitation	**set igmp mrsol** on page 436
	set igmp mrsol mrsi on page 436
Multicast Routers	**set igmp mrouter** on page 435
	display igmp mrouter on page 426
Multicast Receivers	**set igmp receiver** on page 441
	display igmp receiver-table on page 429
Statistics	**display igmp statistics** on page 431
	clear igmp statistics on page 422

Downloaded from www.Manualslib.com manuals search engine

clear igmp statistics

Clears IGMP statistics counters on one VLAN or all VLANs on a wireless LAN switch and resets them to 0.

Syntax — clear igmp statistics [**vlan** *vlan-id*]

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears IGMP statistics for all VLANs:

```
WX1200# clear igmp statistics
IGMP statistics cleared for all vlans
```

See Also — display igmp statistics on page 431

display igmp

Displays IGMP configuration information and statistics.

Syntax — display igmp [**vlan** *vlan-id*]

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP information for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays IGMP information for VLAN *orange*:

```
WX1200# display igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast
```

Downloaded from www.Manualslib.com manuals search engine

```
router information:
Port Mrouter-IPaddr Mrouter-MAC        Type  TTL
---- -------------- ----------------- ----- -----
  1       192.28.7.5 00:01:02:03:04:05 dvmrp    17
Group           Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   258
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   258
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   258
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   258
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
IGMP vlan member ports: 1, 2, 3
IGMP static ports: none
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 75 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 75 Output for display igmp

Field	Description
VLAN	VLAN name. MSS displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.
Proxy reporting	Proxy reporting state.
Mrouter solicitation	Multicast router solicitation state.
Querier functionality	Pseudo-querier state.
Configuration values (qi)	Query interval.
Configuration values (oqi)	Other-querier-present interval.
Configuration values (qri)	Query response interval.
Configuration values (lmqi)	Last member query interval.
Configuration values (rvalue)	Robustness value.
Multicast router information	List of multicast routers and active multicast groups. The fields containing this information are described separately. The **display igmp mrouter** command shows the same information.
Port	Number of the physical port through which the WX can reach the router.
Mrouter-IPaddr	IP address of the multicast router interface.
Mrouter-MAC	MAC address of the multicast router interface.
Type	How the WX learned that the port is a multicast router port: ▪ **conf** — Static multicast port configured by an administrator ▪ **madv** — Multicast advertisement ▪ **quer** — IGMP query ▪ **dvmrp** — Distance Vector Multicast Routing Protocol (DVMRP) ▪ **pimv1** — Protocol Independent Multicast (PIM) version 1 ▪ **pimv2** — PIM version 2

Downloaded from www.Manualslib.com manuals search engine

Table 75 Output for display igmp (continued)

Field	Description
TTL	Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is *undef*. Static multicast router entries do not age out.
Group	IP address of a multicast group. The **display igmp receiver-table** command shows the same information as these receiver fields.
Port	Physical port through which the WX can reach the group's receiver.
Receiver-IP	IP address of the client receiving the group.
Receiver-MAC	MAC address of the client receiving the group.
TTL	Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is *undef*. Static multicast receiver entries do not age out.
Querier information	Information about the subnet's multicast querier. If the querier is another WX switch, the fields described below are applicable. If the querier is the WX itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The **display igmp querier** command shows the same information.
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier.
Querier-MAC	MAC address of the querier.
TTL	Number of seconds before this entry ages out if the WX does not receive a query message from the querier.
IGMP vlan member ports	Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports MSS dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver. For example, the list can include a MAP access port that is not configured to be in the VLAN when a user associated with the 3Com Wireless LAN Managed Access Point AP2750 on that port becomes a receiver for a group. When all receivers on a dynamically added port age out, MSS removes the port from the list.
IGMP static ports	Static receiver ports.
IGMP statistics	Multicast message and packet statistics. These are the same statistics displayed by the **display igmp statistics** command.

Downloaded from www.Manualslib.com manuals search engine

Table 75 Output for display igmp (continued)

Field	Description
VLAN	VLAN name. MSS displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.

See Also

- **display igmp mrouter** on page 426
- **display igmp querier** on page 427
- **display igmp receiver-table** on page 429
- **display igmp statistics** on page 431

display igmp mrouter

Displays the multicast routers in a WX's subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the wireless LAN switch can reach the router.

Syntax — `display igmp mrouter` [`vlan` *vlan-id*]

- **`vlan`** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the multicast routers in VLAN *orange*:

```
WX1200# display igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr  Mrouter-MAC       Type  TTL
---- --------------- ----------------- ----- -----
  1       192.28.7.5 00:01:02:03:04:05 dvmrp    33
```

Table 76 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 76 Output for display igmp mrouter

Field	Description
Multicast routers for vlan	VLAN containing the multicast routers. Ports are listed separately for each VLAN.
Port	Number of the physical port through which the WX can reach the router.
Mrouter-IPaddr	IP address of the multicast router.
Mrouter-MAC	MAC address of the multicast router.
Type	How the WX learned that the port is a multicast router port: ▪ **conf** — Static multicast port configured by an administrator ▪ **madv** — Multicast advertisement ▪ **quer** — IGMP query ▪ **dvmrp** — Distance Vector Multicast Routing Protocol (DVMRP) ▪ **pimv1** — Protocol Independent Multicast (PIM) version 1 ▪ **pimv2** — PIM version 2
TTL	Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is *undef*. Static multicast router entries do not age out.

See Also

- **display igmp mrouter** on page 426
- **set igmp mrouter** on page 435

display igmp querier

Shows information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

Syntax — `display igmp querier` [`vlan` *`vlan-id`*]

- **`vlan`** *`vlan-id`* **—** VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History — Introduced in MSS Version 3.0.

Examples — The following command displays querier information for VLAN *orange*:

```
WX1200# display igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
```

The following command shows the information MSS displays when the querier is the WX itself:

```
WX1200# display igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the WX switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
WX1200# display igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 77 describes the fields in this display. Table 76 on page 427 describes the fields in the display when a querier other than the WX is present.

Table 77 Output for display igmp mrouter

Field	Description
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier interface.
Querier-MAC	MAC address of the querier interface.
TTL	Number of seconds before this entry ages out if the WX does not receive a query message from the querier.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set igmp querier** on page 441

display igmp receiver-table

Displays the receivers to which a WX forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax — **display igmp receiver-table** [**vlan** *vlan-id*] [**group** *group-ip-addr/mask-length*]

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.
- **group** *group-ip-addr/mask-length* — IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays all multicast receivers in VLAN *orange*:

```
WX1200# display igmp receiver-table vlan orange
VLAN: orange
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   179
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   179
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   179
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   179
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   179
```

Downloaded from www.Manualslib.com manuals search engine

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
WX1200# display igmp receiver-table group 237.255.255.0/24
VLAN: red
Session          Port Receiver-IP     Receiver-MAC      TTL
---------------- ---- --------------- ----------------- -----
237.255.255.2      2     10.10.20.19 00:02:04:06:09:0d   112
237.255.255.119    3     10.10.30.31 00:02:04:06:01:0b   112

VLAN: green
Session          Port Receiver-IP     Receiver-MAC      TTL
---------------- ---- --------------- ----------------- -----
237.255.255.17     1     10.10.40.41 00:02:06:08:02:0c    12
237.255.255.255    6     10.10.60.61 00:05:09:0c:0a:01   111
```

Table 78 describes the fields in this display.

Table 78 Output for display igmp receiver-table

Field	Description
VLAN	VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.
Session	IP address of the multicast group being received.
Port	Physical port through which the WX can reach the receiver.
Receiver-IP	IP address of the receiver.
Receiver-MAC	MAC address of the receiver.
TTL	Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is *undef*. Static multicast receiver entries do not age out.

See Also

- **set igmp receiver** on page 441

Downloaded from www.Manualslib.com manuals search engine

display igmp statistics

Shows IGMP statistics.

Syntax — `display igmp statistics` [`vlan` *`vlan-id`*]

- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP statistics for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays IGMP statistics for VLAN *orange*:

```
WX1200# display igmp statistics vlan orange
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 79 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 79 Output of display igmp statistics

Field	Description
IGMP statistics for vlan	VLAN name. Statistics are listed separately for each VLAN.
IGMP message type	Type of IGMP message: ▪ **General-Queries** — General group membership queries sent by the multicast querier (multicast router or pseudo-querier). ▪ **GS-Queries** — Group-specific queries sent by the multicast querier to determine whether there are receivers for a specific group. ▪ **Report V1** — IGMP version 1 group membership reports sent by clients who want to be receivers for the groups. ▪ **Report V2** — IGMP version 2 group membership reports sent by clients who want to be receivers for the groups. ▪ **Leave** — IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2. ▪ **Mrouter-Adv** — Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface. ▪ **Mrouter-Term** — Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown. ▪ **Mrouter-Sol** — Multicast router solicitation messages. A multicast client or a WX sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet. ▪ **DVMRP** — Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages. ▪ **PIM V1** — Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages. ▪ **PIM V2** — PIM version 2 messages.
Received	Number of packets received.
Transmitted	Number of packets transmitted. This number includes both multicast packets originated by the WX and multicast packets received and then forwarded by the WX.
Dropped	Number of IGMP packets dropped by the WX.

Downloaded from www.Manualslib.com manuals search engine

Table 79 Output of display igmp statistics (continued)

Field	Description
Topology notifications	Number of Layer 2 topology change notifications received by the WX. In the current software version, the value in this field is always 0.
Packets with unknown IGMP type	Number of multicast packets received with an unrecognized multicast type.
Packets with bad length	Number of packets with an invalid length.
Packets with bad IGMP checksum	Number of packets with an invalid IGMP checksum value.
Packets dropped	Number of multicast packets dropped by the WX.

See Also

- **clear igmp statistics** on page 422

set igmp

Disables or reenables IGMP snooping on one VLAN or all VLANs on a wireless LAN switch.

Syntax — **`set igmp`** {**`enable`** | **`disable`**} [**`vlan`** *`vlan-id`*]

- **`enable`** — Enables IGMP snooping.
- **`disable`** — Disables IGMP snooping.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

History — Introduced in MSS Version 3.0.

Examples — The following command disables IGMP snooping on VLAN *orange*:

```
WX1200# set igmp disable vlan orange
success: change accepted
```

See Also

- **set igmp rv** on page 442

Downloaded from www.Manualslib.com manuals search engine

set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a wireless LAN switch.

Syntax — `set igmp lmqi` *`tenth-seconds`* [`vlan` *`vlan-id`*]

- **`lmqi`** *`tenth-seconds`* — Amount of time (in tenths of a second) that the WX waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the WX switch also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default last member query interval is 10 tenths of a second (1 second).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the last member query interval on VLAN *orange* to 5 tenths of a second:

```
WX1200# set igmp lmqi 5 vlan orange
success: change accepted.
```

See Also

- **set igmp oqi** on page 437
- **set igmp qi** on page 439
- **set igmp mrouter** on page 435

Downloaded from www.Manualslib.com manuals search engine

set igmp mrouter

Adds or removes a port in a WX's list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax — **`set igmp mrouter port`** *`port-list`* {**`enable`** | **`disable`**}

- **`port`** *`port-list`* — Port list. MSS adds or removes the specified ports in the list of static multicast router ports.
- **`enable`** — Adds the port to the list of static multicast router ports.
- **`disable`** — Removes the port from the list of static multicast router ports.

Defaults — By default, no ports are static multicast router ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 6 as a static multicast router port:

```
WX1200# set igmp mrouter port 6 enable
success: change accepted.
```

The following command removes port 6 from the static multicast router port list:

```
WX1200# set igmp mrouter port 6 disable
success: change accepted.
```

See Also

- **display igmp statistics** on page 431

Downloaded from www.Manualslib.com manuals search engine

set igmp mrsol

Enables or disables multicast router solicitation by a WX.

Syntax — `set igmp mrsol {enable | disable} [vlan vlan-id]`

- **`enable`** — Enables multicast router solicitation.
- **`disable`** — Disables multicast router solicitation.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

Defaults — Multicast router solicitation is disabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables multicast router solicitation on VLAN *orange*:

```
WX1200# set igmp mrsol enable vlan orange
success: change accepted
```

See Also

- **set igmp mrsol mrsi** on page 436

set igmp mrsol mrsi

Changes the interval between multicast router solicitations by a WX on one VLAN or all VLANs.

Syntax — `set igmp mrsol mrsi seconds [vlan vlan-id]`

- **`seconds`** — Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs.

Defaults — The interval between multicast router solicitations is 30 seconds by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following example changes the multicast router solicitation interval to 60 seconds:

```
WX1200# set igmp mrsol mrsi 60
success: change accepted.
```

See Also

- **set igmp mrsol** on page 436.

set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a WX.

Syntax — `set igmp oqi` *`seconds`* [`vlan` *`vlan-id`*]

- **`oqi`** *`seconds`* — Number of seconds that the WX waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default other-querier-present interval is 255 seconds (4.25 minutes).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — A WX cannot become the querier unless the pseudo-querier feature is enabled on the WX switch. When the feature is enabled, the WX becomes the querier for a subnet so long as the WX does not receive a query message from a router with a lower IP address than the IP address of the WX in that subnet. To enable the pseudo-querier feature, use **set igmp querier.**

Examples — The following command changes the other-querier-present interval on VLAN *orange* to 200 seconds:

```
WX1200# set igmp oqi 200 vlan orange
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set igmp lmqi** on page 434
- **set igmp qi** on page 439
- **set igmp qri** on page 440
- **set igmp querier** on page 441
- **set igmp mrouter** on page 435
- **set igmp rv** on page 442

set igmp proxy-report

Disables or reenables proxy reporting by a WX on one VLAN or all VLANs.

Syntax — **set igmp proxy-report** {**enable** | **disable**}

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.
- **enable** — Enables proxy reporting.
- **disable** — Disables proxy reporting.

Defaults — Proxy reporting is enabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the WX sends all membership reports to the routers, including multiple reports for the same group.

Examples — The following example disables proxy reporting on VLAN *orange*:

```
WX1200# set igmp proxy-report disable vlan orange
success: change accepted.
```

See Also

- **set igmp rv** on page 442

Downloaded from www.Manualslib.com manuals search engine

set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a WX.

Syntax — **set igmp qi** *seconds* [**vlan** *vlan-id*]

- **qi** *seconds* — Number of seconds that elapse between general queries sent by the WX when the WX switch is the querier for the subnet. You can specify a value from 1 through 65,535.
- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query interval is 125 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query interval is applicable only when the WX is querier for the subnet. For the WX switch to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use the **set igmp querier** command.

Examples — The following command changes the query interval on VLAN *orange* to 100 seconds:

```
WX1200# set igmp qi 100 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 434
- **set igmp oqi** on page 437
- **set igmp qri** on page 440
- **set igmp querier** on page 441
- **set igmp mrouter** on page 435
- **set igmp rv** on page 442

Downloaded from www.Manualslib.com manuals search engine

set igmp qri

Changes the IGMP query response interval timer on one VLAN or all VLANs on a WX.

Syntax — **set igmp qri** *tenth-seconds* [**vlan** *vlan-id*]

- **qri** *tenth-seconds* — Amount of time (in tenths of a second) that the WX waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.
- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query response interval is 100 tenths of a second (10 seconds).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query response interval is applicable only when the WX is querier for the subnet. For the WX to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use **set igmp querier.**

Examples — The following command changes the query response interval on VLAN *orange* to 50 tenths of a second (5 seconds):

```
WX1200# set igmp qri 50 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 434
- **set igmp oqi** on page 437
- **set igmp qi** on page 439
- **set igmp querier** on page 441
- **set igmp rv** on page 442

Downloaded from www.Manualslib.com manuals search engine

set igmp querier

Enables or disables the IGMP pseudo-querier on a WX, on one VLAN or all VLANs.

Syntax — **`set igmp querier`** {**`enable`** | **`disable`**} [**`vlan`** *`vlan-id`*]

- **`enable`** — Enables the pseudo-querier.
- **`disable`** — Disables the pseudo-querier.
- **`vlan`** *`vlan-id`* — VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

Defaults — The pseudo-querier is disabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — 3Com recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

Examples — The following example enables the pseudo-querier on the *orange* VLAN:

```
WX1200# set igmp querier enable vlan orange
success: change accepted.
```

See Also

- **display igmp querier** on page 427

set igmp receiver

Adds or removes a network port in the list of ports on which a WX forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

Syntax — **`set igmp receiver port`** *`port-list`* {**`enable`** | **`disable`**}

- **`port`** *`port-list`* — Network port list. MSS adds the specified ports to the list of static multicast receiver ports.
- **`enable`** — Adds the port to the list of static multicast receiver ports.
- **`disable`** — Removes the port from the list of static multicast receiver ports.

Downloaded from www.Manualslib.com manuals search engine

Defaults — By default, no ports are static multicast receiver ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 7 as a static multicast receiver port:

```
WX1200# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 7 from the list of static multicast receiver ports:

```
WX1200# set igmp receiver port 7 disable
success: change accepted.
```

See Also

- **display igmp receiver-table** on page 429

set igmp rv

Changes the robustness value for one VLAN or all VLANs on a WX. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

Syntax — **set igmp rv** *num* [**vlan** *vlan-id*]

- *num* — Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss.
- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS changes the robustness value for all VLANs.

Defaults — The default robustness value for all VLANs is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

See Also

- **set igmp oqi** on page 437
- **set igmp qi** on page 439
- **set igmp qri** on page 440

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

14 SECURITY ACL COMMANDS

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on a WX switch, which helps you locally control user access. For location policy commands, see "AAA Commands" on page 201.)

Security ACL Commands by Usage

This chapter presents security ACL commands alphabetically. Use Table 80 to locate commands in this chapter based on their use.

Table 80 Security ACL Commands by Usage

Type	Command
Create Security ACLs	**set security acl** on page 459
	display security acl on page 450
	display security acl info on page 452
	clear security acl on page 446
Commit Security ACLs	**commit security acl** on page 449
	rollback security acl on page 458
Map Security ACLs	**set security acl map** on page 464
	display security acl map on page 453
	clear security acl map on page 447
Monitor Security ACLs	**display security acl hits** on page 451
	set security acl hit-sample-rate on page 466
	display security acl resource-usage on page 454

Downloaded from www.Manualslib.com manuals search engine

clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

Syntax — **clear security acl** {*acl-name* | **all**} [*editbuffer-index*]

- *acl-name* — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
- **all** — Clears all security ACLs.
- *editbuffer-index* — Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

Examples — The following commands display the current security ACL configuration, *clear acl_133* in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to display that it no longer contains *acl_133*:

Downloaded from www.Manualslib.com manuals search engine

```
WX4400# display security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
-------------------------------------------------------
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
-------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
WX4400# clear security acl acl_133
WX4400# commit security acl acl_133
configuration accepted
WX4400# display security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
-------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

See Also

- **clear security acl map** on page 447
- **commit security acl** on page 449
- **display security acl info** on page 452
- **set security acl** on page 459

clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a WX switch.

Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local WX database, use the command ***clear user attr, clear mac-user attr, clear usergroup attr,*** *or* ***clear mac-usergroup attr.*** *To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.*

Downloaded from www.Manualslib.com manuals search engine

Syntax — **clear security acl map** {*acl-name* | **all**} {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-value*] | **dap** *dap-num*} {**in** | **out**}

- *acl-name* — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
- **all** — Removes security ACL mapping from all physical ports, virtual ports, and VLANs on a WX switch.
- **vlan** *vlan-id* — VLAN name or number. MSS removes the security ACL from the specified VLAN.
- **port** *port-list* — Port list. MSS removes the security ACL from the specified WX physical port or ports.
- **tag** *tag-value* — Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port.
- **dap** *dap-num* — One or more Distributed MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS removes the security ACL from the specified Distributed MAPs.
- **in** — Removes the security ACL from traffic coming *into* the WX switch.
- **out** — Removes the security ACL from traffic going *out of* the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed MAP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

Examples — To clear the mapping of security ACL *acljoe* from port 4 for incoming packets, type the following command:

```
WX4400# clear security acl map acljoe port 4 in
clear mapping accepted
```

Downloaded from www.Manualslib.com manuals search engine

To clear all physical ports, virtual ports, and VLANs on a WX switch of the ACLs mapped for incoming and outgoing traffic, type the following command:

```
WX4400# clear security acl map all
success: change accepted.
```

See Also

- **clear security acl** on page 446
- **display security acl map** on page 453
- **set security acl map** on page 464

commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the WX switch. Or, when used with the clear security acl command, **commit security acl** deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

Syntax — **commit security acl** {*acl-name* | **all**}

- *acl-name* — Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.
- **all** — Commits all security ACLs in the edit buffer.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever **display security acl info all editbuffer** shows to be currently stored in the edit buffer.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
WX4400# commit security acl all
configuration accepted
WX4400# display security acl
ACL table
ACL                      Type  Class   Mapping
-----------------------  ----  ------  -------
acl_123                  IP    Static
acl_124                  IP    Static
WX4400# display security acl info all editbuffer
acl editbuffer information for all
```

See Also

- **clear security acl** on page 446
- **display security acl** on page 450
- **display security acl info** on page 452
- **rollback security acl** on page 458
- **set security acl** on page 459

display security acl

Displays a summary of security ACLs that are committed — saved in the running configuration and nonvolatile storage — or a summary of ACLs in the edit buffer.

Syntax — **display security acl** [**editbuffer**]

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — To display a summary of the committed security ACLs on a WX switch, type the following command:

```
WX4400# display security acl
ACL table
ACL                          Type Class  Mapping
---------------------------- ---- ------ -------
acl_123                      IP   Static Port 2 In
acl_133                      IP   Static Port 4 In
acl_124                      IP   Static
```

To view a summary of the security ACLs in the edit buffer, type the following command:

```
WX4400# display security acl editbuffer
ACL edit-buffer table
ACL                          Type Status
---------------------------- ---- --------------
acl_122                      IP   Not committed
acl_132                      IP   Not committed
acl-144                      IP   Not committed
```

See Also

- **clear security acl** on page 446
- **display security acl info** on page 452
- **set security acl** on page 459

display security acl hits

Displays the number of packets filtered by security ACLs ("hits") on the WX switch. Each time a packet is filtered by a security ACL, the hit counter increments.

Syntax — **display security acl hits**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — For MSS to count hits for a security ACL, you must specify hits in the **set security acl** commands that define ACE rules for the ACL.

Downloaded from www.Manualslib.com manuals search engine

Examples — To display the security ACL hits on a WX switch, type the following command:

```
WX4400# display security acl hits
ACL hit-counters
Index Counter              ACL-name
----- -------------------- --------
    1                    0 acl_2
    2                    0 acl_175
    3                  916 acl_123
```

See Also

- **set security acl hit-sample-rate** on page 466
- **set security acl** on page 459

display security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed — saved in the running configuration and nonvolatile storage — or the contents of security ACLs in the edit buffer before they are committed.

Syntax — display security acl info {*acl-name* | **all**] [**editbuffer**]

- *acl-name* — Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
- **all** — Displays the contents of all security ACLs.
- **editbuffer** — Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with **set security acl**. If you do not use this parameter, only committed ACLs are shown.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. The *acl-name* | **all** option is no longer required; **display security acl info** is valid and displays the same information as **security acl info all** in MSS Version 4.1.

Downloaded from www.Manualslib.com manuals search engine

Examples — To display the contents of all security ACLs committed on a WX switch, type the following command:

```
WX4400# display security acl info
ACL information for all
set security acl ip acl_123 (hits #5 462)
------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of *acl_123* in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
WX4400# display security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

See Also

- **clear security acl** on page 446
- **commit security acl** on page 449
- **set security acl** on page 459

display security acl map

Displays the VLANs, ports, and virtual ports on the WX switch to which a security ACL is assigned.

Syntax — **display security acl map** *acl-name*

- *acl-name* — Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the port to which security ACL *acl_111* is mapped:

```
WX4400# display security acl map acl_111
ACL acl_111 is mapped to:
Port 4 in
```

See Also

- **clear security acl map** on page 447
- **display security acl map** on page 453
- **set security acl map** on page 464

display security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the WX switch.

Syntax — **display security acl resource-usage**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command with the help of 3Com to diagnose an ACL resource problem. (To obtain 3Com Technical Support, see "Obtaining Support for your Product" on page 637.)

Downloaded from www.Manualslib.com manuals search engine

Examples — To display security ACL resource usage, type the following command:

```
WX4400# display security acl resource-usage
ACL resources

Classifier tree counters
------------------------
  Number of rules           : 2
  Number of leaf nodes      : 1
  Stored rule count         : 2
  Leaf chain count          : 1
  Longest leaf chain        : 2
  Number of non-leaf nodes  : 0
  Uncompressed Rule Count   : 2
  Maximum node depth        : 1
  Sub-chain count           : 0
  PSCBs in primary memory   : 0 (max: 512)
  PSCBs in secondary memory : 0 (max: 9728)
  Leaves in primary         : 2 (max: 151)
  Leaves in secondary       : 0 (max 12096)
  Sum node depth            : 1
Information on Network Processor status
---------------------------------------
  Fragmentation control     : 0
  UC switchdest             : 0
ACL resources
  Port number               : 0
  Number of action types    : 2
  LUdef in use              : 5
  Default action pointer    : c8007dc
  L4 global                 : True
  No rules                  : False
  Non-IP rules              : False
  Root in first             : True
  Static default action     : False
  No per-user (MAC) mapping : True
  Out mapping               : False
  In mapping                : True
  No VLAN or PORT mapping   : False
  No VPORT mapping          : True
```

Table 81 explains the fields in the **display security acl resource-usage** output.

Downloaded from www.Manualslib.com manuals search engine

Table 81 Output of display security acl resource-usage

Field	Description
Number of rules	Number of security ACEs currently mapped to ports or VLANs.
Number of leaf nodes	Number of security ACL data entries stored in the rule tree.
Stored rule count	Number of security ACEs stored in the rule tree.
Leaf chain count	Number of chained security ACL data entries stored in the rule tree.
Longest leaf chain	Longest chain of security ACL data entries stored in the rule tree.
Number of non-leaf nodes	Number of nodes with no data entries stored in the rule tree.
Uncompressed Rule Count	Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs.
Maximum node depth	Number of data elements in the rule tree, from the root to the furthest data entry (leaf).
Sub-chain count	Sum of action types represented in all security ACL data entries.
PSCBs in primary memory	Number of pattern search control blocks (PSCBs) stored in primary node memory.
PSCBs in secondary memory	Number of PSCBs stored in secondary node memory.
Leaves in primary	Number of security ACL data entries stored in primary leaf memory.
Leaves in secondary	Number of ACL data entries stored in secondary leaf memory.
Sum node depth	Total number of security ACL data entries.
Fragmentation control	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
UC switchdest	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Port number	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Number of action types	Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either *permit* or *deny*.

Downloaded from www.Manualslib.com manuals search engine

Table 81 Output of display security acl resource-usage (continued)

Field	Description
LUdef in use	Number of the lookup definition (LUdef) table currently in use for packet handling.
Default action pointer	Memory address used for packet handling, from which default action data is obtained when necessary.
L4 global	Security ACL mapping on the WX switch: ■ **True** — Security ACLs are mapped. ■ **False** — No security ACLs are mapped.
No rules	Security ACE rule mapping on the WX switch: ■ **True** — No security ACEs are mapped. ■ **False** — Security ACEs are mapped.
Non-IP rules	Non-IP security ACE mapping on the WX switch: ■ **True** — Non-IP security ACEs are mapped. ■ **False** — Only IP security ACEs are mapped. **Note:** The current MSS version supports security ACEs for IP only.
Root in first	Leaf buffer allocation: ■ **True** — Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves. ■ **False** — Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.
Static default action	Definition of a default action: ■ **True** — A default action types is defined. ■ **False** — No default action type is defined.
No per-user (MAC) mapping	Per-user application of a security ACL with the Filter-Id attribute, on the WX switch: ■ **True** — No security ACLs are applied to users. ■ **False** — Security ACLs are applied to users.
Out mapping	Application of security ACLs to outgoing traffic on the WX switch: ■ **True** — Security ACLs are mapped to outgoing traffic. ■ **False** — No security ACLs are mapped to outgoing traffic.

Downloaded from www.Manualslib.com manuals search engine

Table 81 Output of display security acl resource-usage (continued)

Field	Description
In mapping	Application of security ACLs to incoming traffic on the WX switch: ▪ **True** — Security ACLs are mapped to incoming traffic. ▪ **False** — No security ACLs are mapped to incoming traffic.
No VLAN or PORT mapping	Application of security ACLs to WX VLANs or ports on the WX switch: ▪ **True** — No security ACLs are mapped to VLANs or ports. ▪ **False** — Security ACLs are mapped to VLANs or ports.
No VPORT mapping	Application of security ACLs to WX virtual ports on the WX switch: ▪ **True** — No security ACLs are mapped to virtual ports. ▪ **False** — Security ACLs are mapped to virtual ports.

rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

Syntax — **`rollback security acl`** {*`acl-name`* | **`all`**}

- *`acl-name`* — Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.
- **`all`** — Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to *security acl_122*, and show the edit buffer after the rollback:

```
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
------------------------------------------------------
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
WX4400# rollback security acl acl_122
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
```

See Also

- **display security acl** on page 450

set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

By source address

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} *source-ip-addr mask* [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By Layer 4 protocol

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} *protocol-number* {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By IP packets

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} **ip** {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

Downloaded from www.Manualslib.com manuals search engine

By ICMP packets

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} **icmp** {*source-ip-addr mask destination-ip-addr mask* [**type** *icmp-type*] [**code** *icmp-code*] [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By TCP packets

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] |**deny**} **tcp** {*source-ip-addr mask* [**operator port [port2**]] *destination-ip-addr mask* [**operator port [port2**]]} **[precedence** *precedence*] [**tos** *tos*] [**established**] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By UDP packets

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} **udp** {*source-ip-addr mask* [**operator port** [**port2**]] *destination-ip-addr mask* [**operator port** [**port2**]]} [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

- *acl-name* — Security ACL name. ACL names must be unique within the WX switch, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters:
  - Letters *a* through *z* and *A* through *Z*
  - Numbers 0 through 9
  - Hyphen (-), underscore (_), and period (.)

  3Com recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names *acl_123* and *ACL_123*.

In an ACL name, do not include the term ***all, default-action, map, help****, or* ***editbuffer****.*

- **permit** — Allows traffic that matches the conditions in the ACE.
- **cos** *cos* — For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7:
  - 1 or 2—Background. Packets are queued in MAP forwarding queue 4.

Downloaded from www.Manualslib.com manuals search engine

  - 0 or 3—Best effort. Packets are queued in MAP forwarding queue 3.
  - 4 or 5—Video. Packets are queued in MAP forwarding queue 2.

    Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP).
  - 6 or 7—Voice. Packets are queued in MAP forwarding queue 1.

    In MSS Version 3.0, use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic.
- **deny** — Blocks traffic that matches the conditions in the ACE.
- *protocol* — IP protocol by which to filter packets:
  - **ip**
  - **tcp**
  - **udp**
  - **icmp**
  - A protocol number between 0 and 255.

  (For a complete list of IP protocol names and numbers, see www.iana.org/assignments/protocol-numbers.)
- *source-ip-addr mask* — IP address and wildcard mask of the network or host from which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see "Wildcard Masks" on page 26.
- *operator port* [*port2*] — Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on source-ip-addr or destination-ip-addr. Specify one of the following operands and the associated port:
  - **eq** — Packets are filtered for only *port* number.
  - **gt** — Packets are filtered for all ports that are greater than *port* number.
  - **lt** — Packets are filtered for all ports that are less than *port* number.
  - **neq** — Packets are filtered for all ports except *port* number.
  - **range** — Packets are filtered for ports in the range between *port* and *port2*. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number.

Downloaded from www.Manualslib.com manuals search engine

(For a complete list of TCP and UDP port numbers, see www.iana.org/assignments/port-numbers.)

- *destination-ip-addr mask* — IP address and wildcard mask of the network or host to which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see "Wildcard Masks" on page 26.
- **type** *icmp-type* — Filters ICMP messages by type. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
- **code** *icmp-code* — For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
- **precedence** *precedence* — Filters packets by precedence level. Specify a value from 0 through 7:
  - **0** — routine precedence
  - **1** — priority precedence
  - **2** — immediate precedence
  - **3** — flash precedence
  - **4** — flash override precedence
  - **5** — critical precedence
  - **6** — internetwork control precedence
  - **7** — network control precedence
- **tos** *tos* — Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a **tos** value of **9** filters packets with the TOS levels minimum delay (**8**) and minimum monetary cost (**1**).
  - **8** — minimum delay
  - **4** — maximum throughput
  - **2** — maximum reliability
  - **1** — minimum monetary cost
  - **0** — normal
- **established** — For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions.

Downloaded from www.Manualslib.com manuals search engine

- **before** *editbuffer-index* — Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **display security acl editbuffer.**)
- **modify** *editbuffer-index* — Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **display security acl editbuffer.**)
- **hits** — Tracks the number of packets that are filtered based on a security ACL, for all mappings.

Defaults — Permitted packets are assigned to class-of-service (CoS) class 0 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The WX switch does not apply security ACLs until you activate them with the **commit security acl** command and map them to a VLAN, port, or virtual port, or to a user. If the WX switch is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored.

ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use **before *editbuffer-index*** and **modify *editbuffer-index.***

Examples — The following command adds an ACE to security *acl_123* that permits packets from IP address 192.168.1.11/24 and counts the hits:

```
WX4400# set security acl ip acl_123 permit
192.168.1.11 0.0.0.255 hits
```

Downloaded from www.Manualslib.com manuals search engine

The following command adds an ACE to *acl_123* that denies packets from IP address 192.168.2.11:

```
WX4400# set security acl ip acl_123 deny 192.168.2.11
0.0.0.0
```

The following command creates *acl_125* by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp
192.168.0.1 0.0.0.0 192.168.0.2 0.0.0.0 established hits
```

The following command adds an ACE to *acl_125* that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp
192.168.1.1 0.0.0.0 192.168.1.2 0.0.0.0 eq 80 hits
```

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

```
WX4400# commit security acl all
configuration accepted
```

See Also

- **clear security acl** on page 446
- **commit security acl** on page 449
- **display security acl** on page 450

set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed MAP on the WX switch.

To assign a security ACL to a user or group in the local WX database, use the command ***set user attr, set mac-user attr, set usergroup attr,*** *or* ***set mac-usergroup attr*** *with the Filter-Id attribute. To assign a security ACL to a user or group with Filter-Id on a RADIUS server, see the documentation for your RADIUS server.*

Downloaded from www.Manualslib.com manuals search engine

Syntax — **set security acl map** *acl-name* {**Vlan** *vlan-id* | **port** *port-list* [**tag** *tag-list*] | **dap** *dap-num*} {**in** | **out**}

- *acl-name* — Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive.
- **vlan** *vlan-id* — VLAN name or number. MSS assigns the security ACL to the specified VLAN.
- **port** *port-list* — Port list. MSS assigns the security ACL to the specified physical WX port or ports.
- **tag** *tag-list* — One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4095. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified virtual port or ports.
- **dap** *dap-num* — One or more Distributed MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified Distributed MAPs.
- **in** — Assigns the security ACL to traffic coming *into* the WX switch.
- **out** — Assigns the security ACL to traffic coming *from* the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before you can map a security ACL, you must use the **commit security acl** command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or Distributed MAP to filter a flow of packets. If more than one security ACL filters the same traffic, MSS applies only the first ACL match and ignores any other matches.

Examples — The following command maps security ACL *acl_133* to port 4 for incoming packets:

```
WX4400 set security acl map acl_133 port 4 in
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear security acl map** on page 447
- **commit security acl** on page 449
- **set mac-user attr** on page 249
- **set mac-usergroup attr** on page 254
- **set security acl** on page 459
- **set user attr** on page 259
- **set usergroup** on page 261
- **display security acl map** on page 453

---

set security acl hit-sample-rate

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL — or "hits."

Syntax — **`set security acl hit-sample-rate`** *`seconds`*

- *`seconds`* — Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

Defaults — By default, the hits are not sampled.

Access — Enabled.

History — Introduced in MSS Version 3.0. Syntax changed from **hit-sample-rate *seconds*** to **set security acl hit-sample-rate *seconds***, to allow the command to be saved in the configuration file.

Usage — To view counter results for a particular ACL, use the **display security acl info acl-name** command. To view the hits for all security ACLs, use the **display security acl hits** command.

Downloaded from www.Manualslib.com manuals search engine

Examples — The first command sets MSS to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching *security acl_153* were sent since the ACL was mapped.

```
WX4400# set security acl hit-sample-rate 15
WX4400# display security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
-------------------------------------------------------
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits
```

```
WX4400# display security acl hits
ACL hit counters
Index Counter              ACL-name
----- -------------------- -----------
    1                    0 acl_2
    2                    0 acl_175
    3                  916 acl_153
```

See Also

- **display security acl hits** on page 451
- **display security acl info** on page 452

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

15 CRYPTOGRAPHY COMMANDS

Use cryptography commands to configure and manage certificates and public-private key pairs for system authentication. Depending on your network configuration, you must create keys and certificates to authenticate the WX switch to IEEE 802.1X wireless clients for which the WX switch performs authentication, and to 3Com wireless switch manager (3WXM) and Web Manager.

Commands by Usage

This chapter presents cryptography commands alphabetically. Use Table 82 to locate commands in this chapter based on their use.

Table 82 Cryptography Commands by Usage

Type	Command
Encryption Keys	**crypto generate key** on page 473
	display crypto key ssh on page 483
PKCS #7 Certificates	**crypto generate request** on page 474
	crypto ca-certificate on page 470
	display crypto ca-certificate on page 481
	crypto certificate on page 471
	display crypto certificate on page 482
PKCS #12 Certificate	**crypto otp** on page 478
	crypto pkcs12 on page 479
Self-Signed Certificate	**crypto generate self-signed** on page 476

Downloaded from www.Manualslib.com manuals search engine

crypto ca-certificate

Installs a certificate authority's own PKCS #7 certificate into the WX certificate and key storage area.

Syntax — **crypto ca-certificate** {**admin** | **eap** | **web**} *PEM-formatted certificate*

- **admin** — Stores the certificate authority's certificate that signed the administrative certificate for the WX switch.

  The administrative certificate authenticates the WX to 3Com wireless switch manager (3XWM) or Web Manager.

- **eap** — Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch.

  The EAP certificate authenticates the WX to 802.1X supplicants (clients).

- **web** — Stores the certificate authority's certificate that signed the WebAAA certificate for the WX switch.

  The Web certificate authenticates the WX to clients who use WebAAA.

- *PEM-formatted certificate* — ASCII text representation of the certificate authority PKCS #7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Downloaded from www.Manualslib.com manuals search engine

To use this command, you must already have obtained a copy of the certificate authority's certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the **crypto ca-certificate** command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

Examples — The following command adds the certificate authority's certificate to WX certificate and key storage:

```
WX4400# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4PO5FAQCyewU3ojANBgkqhkiG9wOBAQUFADCB
mzerMClaweVQQTTooewi\wpoer0QWNFNkj90044mbdrl1277SWQ8G7DiwYUtrqoQplKJvxz
.....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also

- **display crypto ca-certificate** on page 481

crypto certificate

Installs one of the WX switch's PKCS #7 certificates into the certificate and key storage area on the WX switch. The certificate, which is issued and signed by a certificate authority, authenticates the WX switch either to 3WXM or Web Manager, or to 802.1X supplicants (clients).

Syntax — **crypto certificate** {**admin** | **eap** | **web**} PEM-formatted certificate

- **admin** — Stores the certificate authority's administrative certificate, which authenticates the WX switch to 3WXM or Web Manager.
- **eap** — Stores the certificate authority's Extensible Authentication Protocol (EAP) certificate, which authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Stores the certificate authority's WebAAA certificate, which authenticates the WX to clients who use WebAAA.

Downloaded from www.Manualslib.com manuals search engine

- *PEM-formatted certificate* — ASCII text representation of the PKCS #7 certificate, consisting of up to 5120 characters, that you have obtained from the certificate authority.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must already have generated a certificate request with the **crypto generate request** command, sent the request to the certificate authority, and obtained a signed copy of the WX switch certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the **crypto certificate** command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

   The WX switch verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the WX switch's private key and the public key in the installed certificate.

Examples — The following command installs a certificate:

```
WX4400# crypto certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQOExGjAYBgNVBAMU
EXR1Y2hwdWJzQHRycHouY29tMIGfMAOGCSqGSIb3DQEBAQAA4GNADCBiQKBgQC4
.....
2L8Q9tk+G2As84QYLm8wmVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also

- **crypto generate request** on page 474
- **crypto generate self-signed** on page 476

Downloaded from www.Manualslib.com manuals search engine

crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, the command generates an SSH authentication key.

Syntax — **crypto generate key** {**admin** | **eap** | **ssh** | **web**} {**512** | **1024** | **2048**}

- **admin** — Generates an administrative key pair for authenticating the WX switch to 3WXM or Web Manager.
- **eap** — Generates an EAP key pair for authenticating the WX switch to 802.1X supplicants (clients).
- **ssh** — Generates a key pair for authenticating the WX switch to Secure Shell (SSH) clients.
- **web** — Generates an administrative key pair for authenticating the WX switch to WebAAA clients.
- **512** | **1024** | **2048** — Length of the key pair in bits.

  The minimum key size for SSH is 1024.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to web in MSS Version 4.1.

Usage — You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on a WX switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

Examples — To generate an administrative key for use with 3WXM, type the following command:

```
WX4400# crypto generate key admin 1024
key pair generated
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display crypto key ssh** on page 483

crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS #10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with 3WXM and Web Manager, or an EAP CSR for use with 802.1X clients.

Syntax — **crypto generate request** {**admin** | **eap** | **web**}

- **admin** — Generates a request for an administrative certificate to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Generates a request for an EAP certificate to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Generates a request for a WebAAA certificate to authenticate the WX switch to WebAAA clients.

After you type the command, you are prompted for the following variables:

- **Country Name** *string* — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.
- **State Name** *string* — (Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.
- **Locality Name** *string* — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
- **Organizational Name** *string* — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
- **Organizational Unit** *string* — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
- **Common Name** *string* — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.

Downloaded from www.Manualslib.com manuals search engine

- **Email Address string** — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
- **Unstructured Name** *string* — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Enter **crypto generate request admin**, **crypto generate request eap**, or **crypto generate request web** and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the WX switch.

This command outputs a PKCS #10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the WX switch certificate as a PKCS #7 object file.

Examples — To request an administrative certificate from a certificate authority, type the following command:

```
WX4400# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Pleasanton
Organizational Name: MyCorp
Organizational Unit: ENG
Common Name: ENG
Email Address: admin@example.com
Unstructured Name: admin
CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwezELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAmNhMQswCQYDVQQH
EwJjYTELMAkGA1UEChMCY2ExCzAJBgNVBAsTAmNhMQswCQYDVQQDEwJjYTEYMBYG
CSqGSIb3DQEJARYJY2FAY2EuY29tMREwDwYJKoZIhvcNAQkCEwJjYTCBnzANBgkq
```

Downloaded from www.Manualslib.com manuals search engine

```
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1zatpYStOjHMa0QJmWHeZPPFGQ9kBEimJKPG
bznFjAC780GcZtnJPGqnMnOKj/4NdknonT6NdCd2fBdGbuEFGNMNgZMYKGcV2JIu
M32SvpSEOEnMYuidkEzqLQol621vh67RM1KTMECM6uCBBROq6XNypIHn1gtrrpL/
LhyGTWUCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAHK5z2kfjBbV/F0b0MyC5S7K
htsw7T4SwmCij55qfUHxsRelggYcw6vJtr57jJ7wFfsMd8C50NcbJLF1nYC9OKkB
hW+5gDPAOZdOnnr591XKz3Zzyvyrktv00rcld8Fo2RtTQ3AOT9cUZqJVelO85GXJ
-----END CERTIFICATE REQUEST-----
```

See Also

- **crypto certificate** on page 471
- **crypto generate key** on page 473

---

crypto generate self-signed

Generates a self-signed certificate for either an administrative certificate for use with 3WXM or an EAP certificate for use with 802.1X wireless users.

Syntax — **crypto generate self-signed** {**admin** | **eap** | **web**}

- **admin** — Generates an administrative certificate to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Generates an EAP certificate to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Generates a WebAAA certificate to authenticate the WX switch to WebAAA clients.

After you type the command, you are prompted for the following variables:

- **Country Name** *string* — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.
- **State Name** *string* — (Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.
- **Locality Name** *string* — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
- **Organizational Name** *string* — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.

Downloaded from www.Manualslib.com manuals search engine

- **Organizational Unit** *string* — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
- **Common Name** *string* — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.

  Note: If you are generating a WebAAA (web) certificate, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use common.name instead of common name. The string is not required to be an actual domain name. It simply needs to be formatted like one.
- **Email Address** *string* — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
- **Unstructured Name** *string* — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

To generate a self-signed administrative certificate, type the following command:

```
WX4400# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name: wx1@example.com
Email Address:
Unstructured Name:
success: self-signed cert for admin generated
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **crypto certificate** on page 471
- **crypto generate key** on page 473

---

crypto otp

Sets a one-time password (OTP) for use with the **crypto pkcs12** command.

Syntax — **crypto otp** {**admin** | **eap** | **web**} *one-time-password*

- **admin** — Creates a one-time password for installing a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Creates a one-time password for installing a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Creates a one-time password for installing a PKCS #12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to WebAAA clients.
- *one-time-password* — Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file.

  Note: On an WX switch that handles communications to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

  The following characters *cannot* be used as part of the one-time password of a PKCS #12 file:

  - Quotation marks (" ")
  - Question mark (?)
  - Ampersand (&)

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. MSS erases the one-time password after processing the **crypto pkcs12** command or when you reboot the WX switch.

3Com recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

Examples — The following command creates the one-time password *hap9iN#ss* for installing an EAP certificate and key pair:

```
WX4400# crypto generate otp eap hap9iN#ss
OTP set
```

See Also

- **crypto pkcs12** on page 479

crypto pkcs12

Unpacks a PKCS #12 object file into the certificate and key storage area on the WX switch. This object file contains a public-private key pair, an WX certificate signed by a certificate authority, and the certificate authority's certificate.

Syntax — **crypto pkcs12** {**admin** | **eap** | **web**} *file-location-url*

- **admin** — Unpacks a PKCS #12 object file for an administrative certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 3WXM or Web Manager.
- **eap** — Unpacks a PKCS #12 object file for an EAP certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 802.1X supplicants (clients).
- **web** — Unpacks a PKCS #12 object file for a WebAAA certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to WebAAA clients.
- *file-location-url* — Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS #12 file.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the WX switch.

Examples — The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the WX switch, create the one-time password *hap9iN#ss*, and unpack the PKCS #12 file:

```
WX4400# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517
bytes/sec]
WX4400# crypto otp eap hap9iN#ss
OTP set
WX4400# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```

See Also

- **crypto otp** on page 478

Downloaded from www.Manualslib.com manuals search engine

display crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

Syntax — **`display crypto ca-certificate`** {**`admin`** | **`eap`** | **`web`**}

- **`admin`** — Displays information about the certificate authority's certificate that signed the administrative certificate for the WX switch.

  The administrative certificate authenticates the WX to 3WXM or Web Manager.

- **`eap`** — Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch.

  The EAP certificate authenticates the WX switch to 802.1X supplicants (clients).

- **`web`** — Displays information about the certificate authority's certificate that signed the WebAAA certificate for the WX switch.

  The WebAAA certificate authenticates the WX switch to WebAAA clients.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to web in MSS Version 4.1.

Examples — To display information about the certificate of a certificate authority, type the following command:

```
WX4400# display crypto ca-certificate
```

Table 83 describes the fields in the display.

Table 83 display crypto ca-certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.

Downloaded from www.Manualslib.com manuals search engine

Table 83 display crypto ca-certificate Output (continued)

Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- **crypto ca-certificate** on page 470
- **display crypto certificate** on page 482

display crypto certificate

Displays information about one of the cryptographic certificates installed on the WX switch.

Syntax — **`display crypto certificate`** {**`admin`** | **`eap`** | **`web`**}

- **`admin`** — Displays information about the administrative certificate that authenticates the WX switch to 3WXM or Web Manager.
- **`eap`** — Displays information about the EAP certificate that authenticates the WX switch to 802.1X supplicants (clients).
- **`web`** — Displays information about the WebAAA certificate that authenticates the WX switch to WebAAA clients.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

Examples — To display information about a cryptographic certificate, type the following command:

```
WX4400# display crypto certificate eap
```

Table 84 describes the fields of the display.

Downloaded from www.Manualslib.com manuals search engine

Table 84 crypto certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- **crypto generate self-signed** on page 476
- **display crypto ca-certificate** on page 481

display crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a *fingerprint*) of the public SSH authentication key. When you connect to the WX switch with an SSH client, you can compare the SSH key checksum displayed by the WX switch with the one displayed by the client to verify that you really are connected to the WX switch and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Syntax — **`display crypto key ssh`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To display SSH key information, type the following command:

```
WX4400# display crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

See Also **crypto generate key** on page 473

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

16 RADIUS and Server Group Commands

Use RADIUS commands to set up communication between a WX switch and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users.

Commands by Usage

This chapter presents RADIUS commands alphabetically. Use Table 85 to locate commands in this chapter based on their uses.

Table 85 RADIUS Commands by Usage

Type	Command
RADIUS Client	**set radius client system-ip** on page 491
	clear radius client system-ip on page 487
RADIUS Servers	**set radius** on page 490
	set radius server on page 494
	clear radius on page 486
	clear radius server on page 489
Server Groups	**set server group** on page 496
	set server group load-balance on page 497
	clear server group on page 489
RADIUS Proxy	**set radius proxy client** on page 492
	set radius proxy port on page 493
	clear radius proxy client on page 488
	clear radius proxy port on page 488

(For information about RADIUS attributes, see the RADIUS appendix in the *Wireless LAN Switch and Controller Configuration Guide*.)

Downloaded from www.Manualslib.com manuals search engine

clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

Syntax — **clear radius** {**deadtime** | **key** | **retransmit** | **timeout** }

- **deadtime** — Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server.
- **key** — Password (shared secret key) used to authenticate to the RADIUS server.
- **retransmit** — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable.
- **timeout** — Number of seconds to wait for the RADIUS server to respond before retransmitting.

Defaults — Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To override the globally set values on a particular RADIUS server, use the **set radius serve**r command.

Examples — To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
WX4400# clear radius deadtime
success: change accepted.
WX4400# clear radius key
success: change accepted.
WX4400# clear radius retransmit
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

```
WX4400# clear radius timeout
success: change accepted.
```

See Also

- **set radius** on page 490
- **set radius server** on page 494
- **display aaa** on page 219

clear radius client system-ip

Removes the WX switch's system IP address from use as the permanent source address in RADIUS client requests from the switch to its RADIUS server(s).

Syntax — **`clear radius client system-ip`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The **clear radius client system-ip** command causes the WX switch to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The WX switch selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the switch.

Examples — To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
WX4400# clear radius client system-ip
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set radius client system-ip** on page 491

Downloaded from www.Manualslib.com manuals search engine

clear radius proxy client

Removes RADIUS proxy client entries for third-party APs.

Syntax — **`clear radius proxy client all`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Examples — The following command clears all RADIUS proxy client entries from the switch:

```
WX4400# clear radius proxy client all
success: change accepted.
```

See Also

- **set radius proxy client** on page 492

clear radius proxy port

Removes RADIUS proxy ports configured for third-party APs.

Syntax — **`clear radius proxy port all`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Examples — The following command clears all RADIUS proxy port entries from the switch:

```
WX4400# clear radius proxy port all
success: change accepted.
```

See Also

- **set radius proxy port** on page 493

Downloaded from www.Manualslib.com manuals search engine

clear radius server

Removes the named RADIUS server from the WX configuration.

Syntax — **`clear radius server`** *`server-name`*

- *`server-name`* — Name of a RADIUS server configured to perform remote AAA services for the WX switch.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command removes the RADIUS server *rs42* from a list of remote AAA servers:

```
WX4400# clear radius server rs42
success: change accepted.
```

See Also

- **display aaa** on page 219
- **set radius server** on page 494

clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

Syntax — **`clear server group`** *`group-name`* [**`load-balance`**]

- *`group-name`* — Name of a RADIUS server group configured to perform remote AAA services for WX switches.
- **`load-balance`** — Ability of group members to share demand for services among servers.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

Downloaded from www.Manualslib.com manuals search engine

Examples — To remove the server group *sg-77* type the following command:

```
WX4400# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group *shorebirds*, type the following command:

```
WX4400# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- **set server group** on page 496

set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the WX switch automatically sets all these values except the password (key).

Syntax — **set radius** {**deadtime** *minutes* | **key** *string* | **retransmit** *number* | **timeout** *seconds*}

- **deadtime** *minutes* — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.
- **key** *string* — Password (shared secret key) used to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 32 characters long, with no spaces or tabs.
- **retransmit** *number* — Number of transmission attempts the WX switch makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
- **timeout** *seconds* — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

Defaults — Global RADIUS parameters have the following default values:

- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key** — No key

Downloaded from www.Manualslib.com manuals search engine

- **retransmit** — 3 (the total number of attempts, including the first attempt)
- **timeout** — 5 seconds

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can specify only one parameter per command line.

Examples — The following commands sets the dead time to 5 minutes, the RADIUS key to *goody*, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the WX switch:

```
WX1200# set radius deadtime 5
success: change accepted.
WX1200# set radius key goody
success: change accepted.
WX1200# set radius retransmit 1
success: change accepted.
WX1200# set radius timeout 21
success: change accepted.
```

See Also

- **clear radius server** on page 489
- **display aaa** on page 219
- **set radius server** on page 494

set radius client system-ip

Causes all RADIUS requests to be sourced from the IP address specified by the **set system ip-addres**s command, providing a permanent source IP address for RADIUS packets sent from the WX switch.

Syntax — **`set radius client system-ip`**

Defaults — None. If you do not use this command, RADIUS packets leaving the WX have the source IP address of the outbound interface, which can change as routing conditions change.

Examples — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — The WX system IP address must be set before you use this command.

Examples — The following command sets the WX system IP address as the address of the RADIUS client:

```
WX4400# set radius client system-ip
success: change accepted.
```

See Also

- **clear radius client system-ip** on page 487
- **set system idle-timeout** on page 58

set radius proxy client

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP ports on which the WX switch listens for RADIUS traffic from the AP.

Syntax — **set radius proxy client address** *ip-address* **[acct-port** *acct-udp-port-number***] [port** *udp-port-number***] key** *string*

- **address** *ip-address* — IP address of the third-party AP. Enter the address in dotted decimal notation.
- **port** *udp-port-number* — UDP port on which the WX switch listens for RADIUS access-requests from the AP.
- **acct-port** *acct-udp-port-number* — UDP port on which the WX switch listens for RADIUS stop-accounting records from the AP.
- **key** *string* — Password (shared secret key) the WX switch uses to authenticate and encrypt RADIUS communication.

Defaults — The default UDP port number for access-requests is 1812. The default UDP port number for stop-accounting records is 1813.

Access — Enabled.

History —Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP ports 1812 and 1813 on the WX:

```
WX4400# set radius proxy client address 10.20.20.9 key
radkey1
success: change accepted.
```

See Also

- **clear radius proxy client** on page 488
- **set authentication proxy** on page 241
- **set radius proxy port** on page 493

set radius proxy port

Configures the WX port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

Syntax — **set radius proxy port** *port-list* **[tag** *tag-value***] ssid** *ssid-name*

- **port** *port-list* — WX port(s) connected to the third-party AP.
- **tag** *tag-value* — 802.1Q tag value in packets sent by the third-party AP for the SSID.
- **ssid** *ssid-name* — SSID supported by the third-party AP.

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.

Enter a separate command for each SSID, and its tag value, you want the WX to support.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command maps SSID *mycorp* to packets received on port 3 or 4, using 802.1Q tag value 104:

```
WX4400# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

See Also

- **clear radius proxy port** on page 488
- **set authentication proxy** on page 241
- **set radius proxy client** on page 492

set radius server

Configures RADIUS servers and their parameters. By default, the WX switch automatically sets all these values except the password (key).

Syntax — **set radius server** *server-name* [**address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**deadtime** *minutes*] [**key** *string*] [**author-password** *password*]

- *server-name* — Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks.
- **address** *ip-address* — IP address of the RADIUS server. Enter the address in dotted decimal notation.
- **auth-port** *port-number* — UDP port that the WX switch uses for authentication and authorization.
- **acct-port** *port-number* — UDP port that the WX switch uses for accounting.
- **timeout** *seconds* — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds.
- **retransmit** *number* — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
- **deadtime** *minutes* — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available.

Downloaded from www.Manualslib.com manuals search engine

- **key** *string* — Password (shared secret key) the WX switch uses to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 32 characters long, with no spaces or tabs.
- **author-password** *password* — Password used for authorization to a RADIUS server for MAC users. Specify a password of up to 32 alphanumeric characters with no spaces or tabs.

Defaults — Default values are listed below:

- **auth-port** — UDP port 1812
- **acct-port** — UDP port 1813
- **timeout** — 5 seconds
- **retransmit** — 3 (the total number of attempts, including the first attempt)
- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key** — No key
- **author-password** — When using RADIUS for authentication, a MAC user's MAC address is also used as the default authorization password for that user, and no global authorization password is set. A last-resort user's default authorization password is *3Com*.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the WX switch, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.

Downloaded from www.Manualslib.com manuals search engine

Examples — To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, and a key string of *keys4u*, type the following command:

```
WX1200# set radius server RS42 address 198.162.1.1 timeout 30
retransmit 2 deadtime 5 key keys4U
```

See Also

- **display aaa** on page 219
- **set authentication admin** on page 229
- **set authentication console** on page 231
- **set authentication dot1x** on page 233
- **set authentication last-resort** on page 236
- **set authentication mac** on page 239
- **set authentication web** on page 242
- **set radius** on page 490
- **set server group** on page 496

set server group

Configures a group of one to four RADIUS servers.

Syntax — **set server group** *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

- *group-name* — Server group name of up to 32 characters, with no spaces or tabs.
- **members** *server-name1, server-name2, server-name3, server-name4* — The names of one or more configured RADIUS servers. You can enter up to four server names.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Downloaded from www.Manualslib.com manuals search engine

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples — To set server group *shorebirds* with members *heron*, *egret*, and *sandpiper*, type the following command:

```
WX1200# set server group shorebirds members heron egret
sandpiper
success: change accepted.
```

See Also

- **clear server group** on page 489
- **display aaa** on page 219
- **set server group load-balance** on page 497

set server group load-balance

Enables or disables load balancing among the RADIUS servers in a server group.

Syntax — **set server group** *group-name* **load-balance** {**enable** | **disable**}

- *group-name* — Server group name of up to 32 characters.
- **load-balance enable** | **disable** — Enables or disables load balancing of authentication requests among the servers in the group.

Defaults — Load balancing is disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can optionally enable load balancing after assigning the server group members. If you configure load balancing, MSS sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, MSS moves to the next method configured with **set authentication** and **set accounting**.

In contrast, if load balancing is *not* configured, MSS always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.

Downloaded from www.Manualslib.com manuals search engine

Examples — To enable load balancing between the members of server group *shorebirds*, type the following command:

```
WX1200# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between *shorebirds* server group members, type the following command:

```
WX1200# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- **clear server group** on page 489
- **clear radius server** on page 489
- **display aaa** on page 219
- **set server group** on page 496

Downloaded from www.Manualslib.com manuals search engine

17 802.1X MANAGEMENT COMMANDS

Use 802. IEEE X management commands to modify the default settings for IEEE 802.1X sessions on an WX switch. For best results, change the settings only if you are aware of a problem with the WX switch's 802.1X performance.

CAUTION: *802.1X parameter settings are global for all SSIDs configured on the switch.*

Commands by Usage

This chapter presents 802.1X commands alphabetically. Use Table 86 to locate commands in this chapter based on their use. For information about configuring 802.1X commands for user authentication, see "AAA Commands" on page 201.

Table 86 802.1X Commands by Usage

Type	Command
Wired Authentication Port Control	**set dot1x port-control** on page 512
	clear dot1x port-control on page 501
	set dot1x authcontrol on page 508
Keys	**set dot1x key-tx** on page 510
	set dot1x tx-period on page 516
	clear dot1x tx-period on page 505
	set dot1x wep-rekey on page 517
	set dot1x wep-rekey-period on page 518
Bonded Authentication	**clear dot1x bonded-period** on page 500
	set dot1x bonded-period on page 509
Reauthentication	**set dot1x reauth** on page 513
	set dot1x reauth-max on page 514

Downloaded from www.Manualslib.com manuals search engine

Table 86 802.1X Commands by Usage (continued)

Type	Command
Reauthentication, cont.	**clear dot1x reauth-max** on page 503
	set dot1x reauth-period on page 515
	clear dot1x reauth-period on page 503
Retransmission	**set dot1x max-req** on page 511
	clear dot1x max-req on page 501
Quiet Period and Timeouts	**set dot1x quiet-period** on page 513
	clear dot1x quiet-period on page 502
	set dot1x timeout auth-server on page 515
	clear dot1x timeout auth-server on page 504
	set dot1x timeout supplicant on page 516
	clear dot1x timeout supplicant on page 504
Settings, Active Clients, and Statistics	**display dot1x** on page 505

clear dot1x bonded-period

Resets the Bonded Auth™ (bonded authentication) period to its default value. The bonded period is the number of seconds MSS retains session information for an authenticated machine while waiting for an 802.1X client on the machine to start (re)authentication for the user. When bonded authentication is enabled, it applies only to an 802.1X user whose authentication rule on the WX switch contains the **bonded** option.

Syntax — **`clear dot1x bonded-period`**

Defaults — The default bonded authentication period is 0 seconds, which disables the feature.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To reset the Bonded period to its default, type the following command:

```
WX4400# clear dot1x bonded-period
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display dot1x** on page 505
- **set dot1x bonded-period** on page 509

clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the WX switch retransmits to a supplicant (client).

Syntax — **`clear dot1x max-req`**

Defaults — The default number is 20.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To reset the number of 802.1X requests the WX can send to the default setting, type the following command:

```
WX4400# clear dot1x max-req
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x max-req** on page 511

clear dot1x port-control

Resets all wired authentication ports on the WX switch to default 802.1X authentication.

Syntax — **`clear dot1x port-control`**

By default, all wired authentication ports are set to **auto** and they process authentication requests as determined by the **set authentication dot1X** command.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — This command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the method configured. This command applies only to wired authentication ports.

Examples — Type the following command to reset the wired authentication port control:

```
WX4400# clear dot1x port-control
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x port-control** on page 512

clear dot1x quiet-period

Resets the quiet period after a failed authentication to the default setting.

Syntax — **clear dot1x quiet-period**

Defaults — The default is 60 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to reset the 802.1X quiet period to the default:

```
WX4400# clear dot1x quiet-period
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x quiet-period** on page 513

Downloaded from www.Manualslib.com manuals search engine

clear dot1x reauth-max

Resets the maximum number of reauthorization attempts to the default setting.

Syntax — **`clear dot1x reauth-max`**

Defaults — The default is 2 attempts.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to reset the maximum number of reauthorization attempts to the default:

```
WX4400# clear dot1x reauth-max
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x reauth-max** on page 514

clear dot1x reauth-period

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

Syntax — **`clear dot1x reauth-period`**

Defaults — The default is 3600 seconds (1 hour).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to reset the default reauthentication time period:

```
WX4400# clear dot1x reauth-period
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x reauth-period** on page 515

Downloaded from www.Manualslib.com manuals search engine

clear dot1x timeout auth-server

Resets to the default setting the number of seconds that must elapse before the WX times out a request to a RADIUS server.

Syntax — **`clear dot1x timeout auth-server`**

Defaults — The default is 30 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To reset the default timeout for requests to an authentication server, type the following command:

```
WX4400# clear dot1x timeout auth-server
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x timeout auth-server** on page 515

clear dot1x timeout supplicant

Resets to the default setting the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

Syntax — **`clear dot1x timeout supplicant`**

Defaults — The default for the authentication timeout sessions is 30 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to reset the timeout period for an authentication session:

```
WX4400# clear dot1x timeout supplicant
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x timeout supplicant** on page 516

Downloaded from www.Manualslib.com manuals search engine

clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the WX switch retransmits an EAP over LAN (EAPoL) packet.

Syntax — **`clear dot1x tx-period`**

Defaults — The default is 5 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to reset the EAPoL retransmission time:

```
WX4400# clear dot1x tx-period
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **set dot1x tx-period** on page 516

display dot1x

Displays 802.1X client information for statistics and configuration settings.

Syntax — **`display dot1x`** {**`clients`** | **`stats`** | **`config`**}

- **`clients`** — Displays information about active 802.1X clients, including client name, MAC address, and state.
- **`stats`** — Displays global 802.1X statistics associated with connecting and authenticating.
- **`config`** — Displays a summary of the current configuration.

Defaults — None.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0. Format of 802.1X authentication rule information in **`display dot1x config`** output changed in MSS Version 3.2. The rules are still listed at the top of the display, but more information is shown for each rule.

Examples — Type the following command to display the 802.1X clients:

```
WX4400# display dot1x clients
MAC Address               State        Vlan             Identity
  -------------             -------      ------           ----------
00:20:a6:48:01:1f       Connecting      (unknown)
00:05:3c:07:6d:7c       Authenticated   vlan-it          EXAMPLE\jose
00:05:5d:7e:94:83       Authenticated   vlan-eng         EXAMPLE\singh
00:02:2d:86:bd:38       Authenticated   vlan-eng         bard@xmple.com
00:05:5d:7e:97:b4       Authenticated   vlan-eng         EXAMPLE\havel
00:05:5d:7e:98:1a       Authenticated   vlan-eng         EXAMPLE\nash
00:0b:be:a9:dc:4e       Authenticated   vlan-pm          xalik@xmple.com
00:05:5d:7e:96:e3       Authenticated   vlan-eng         EXAMPLE\mishan
00:02:2d:6f:44:77       Authenticated   vlan-eng         EXAMPLE\ethan
00:05:5d:7e:94:89       Authenticated   vlan-eng         EXAMPLE\fmarshall
00:06:80:00:5c:02       Authenticated   vlan-eng         EXAMPLE\bmccarthy
00:02:2d:6a:de:f2       Authenticated   vlan-pm          neailey@xmple.com
00:02:2d:5e:5b:76       Authenticated   vlan-pm          EXAMPLE\tamara
00:02:2d:80:b6:e1       Authenticated   vlan-cs          dmc@xmple.com
00:30:65:16:8d:69       Authenticated   vlan-wep         MAC authenticated
00:02:2d:64:8e:1b       Authenticated   vlan-eng         EXAMPLE\wong
```

Type the following command to display the 802.1X configuration:

```
WX1200# display dot1x config

        802.1X user policy
       ----------------------
        'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
        'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)
```

Downloaded from www.Manualslib.com manuals search engine

```
802.1X parameter                setting
----------------                -------
supplicant timeout              30
auth-server timeout             30
quiet period                    5
transmit period                 5
reauthentication period         3600
maximum requests                2
key transmission                enabled
reauthentication                enabled
authentication control          enabled
WEP rekey period                1800
WEP rekey                       enabled
Bonded period                   60

port 5, authcontrol: auto, max-sessions: 16
port 6, authcontrol: auto, max-sessions: 1
port 7, authcontrol: auto, max-sessions: 1
port 8, authcontrol: auto, max-sessions: 1
```

Type the following command to display 802.1X statistics:

```
WX4400# display dot1x stats
        802.1X statistic                value
        ----------------                -----
        Enters Connecting:              709
        Logoffs While Connecting:       112
        Enters Authenticating:          467
        Success While Authenticating:   0
        Timeouts While Authenticating:  52
        Failures While Authenticating:  0
        Reauths While Authenticating:   0
        Starts While Authenticating:    31
        Logoffs While Authenticating:   0
        Starts While Authenticated:     85
        Logoffs While Authenticated:    1
        Bad Packets Received:           0
```

Table 87 explains the counters in the **display dot1x stats** output.

Downloaded from www.Manualslib.com manuals search engine

Table 87 display dot1x stats Output

Field	Description
Enters Connecting	Number of times that the WX switch state transitions to the CONNECTING state from any other state.
Logoffs While Connecting	Number of times that the WX switch state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message.
Enters Authenticating	Number of times that the state wildcard transitions.
Success While Authenticating	Number of times the WX switch state transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client).
Timeouts While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING.
Failures While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATION to HELD.
Reauths While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Starts While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client).
Logoffs While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client).
Bad Packets Received	Number of EAPoL packets received that have an invalid version or type.

set dot1x authcontrol

Provides a global override mechanism for 802.1X authentication configuration on wired authentication ports.

Syntax — **`set dot1x authcontrol`** {**`enable`** | **`disable`**}

- **`enable`** — Allows all wired authentication ports running 802.1X to use the authentication specified per port by the **set dot1X port-control** command.
- **`disable`** — Forces all wired authentication ports running 802.1X to unconditionally accept all 802.1X authentication attempts with an EAP Success message (ForceAuth).

Downloaded from www.Manualslib.com manuals search engine

Defaults — By default, authentication control for individual wired authentication is enabled.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command applies only to wired authentication ports.

Examples — To enable per-port 802.1X authentication on wired authentication ports, type the following command:

```
WX4400# set dot1x authcontrol enable
success: dot1x authcontrol enabled.
```

See Also

- **display dot1x** on page 505
- **set dot1x port-control** on page 512

set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period, which is the number of seconds MSS retains session information for an authenticated machine while waiting for the 802.1X client on the machine to start (re)authentication for the user.

You must set the bonded period to longer than 0 seconds to enable bonded authentication.

Syntax — **`set dot1x bonded-period`** *`seconds`*

- *`seconds`* — Number of seconds MSS retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds.

Defaults — The default bonded period is 0 seconds, which disables the feature.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

3Com recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

The bonded authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

Examples — To set the bonded authentication period to 60 seconds, type the following command:

```
WX4400# set dot1x bonded-period 60
success: change accepted.
```

See Also

- **display dot1x** on page 505
- **clear dot1x bonded-period** on page 500

set dot1x key-tx

Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

Syntax — **set dot1x key-tx** {**enable** | **disable**}

- **enable** — Enables transmission of encryption key information to clients.
- **disable** — Disables transmission of encryption key information to clients.

Defaults — Key transmission is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — Type the following command to enable key transmission:

```
WX4400# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

See Also

- **display dot1x** on page 505

set dot1x max-req

Sets the maximum number of times the WX retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax — **set dot1x max-req** *number-of-retransmissions*

- *number-of-retransmissions* — Specify a value between 0 and 10.

Defaults — The default number of EAP retransmissions is 2.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Examples — Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
WX4400# set dot1x max-req 3
success: dot1x max request set to 3.
```

See Also

- **clear dot1x max-req** on page 501
- **display dot1x** on page 505

Downloaded from www.Manualslib.com manuals search engine

set dot1x port-control

Determines the 802.1X authentication behavior on individual wired authentication ports or groups of ports.

Syntax — **`set dot1x port-control`**
`{forceauth` | **`forceunauth`** | **`auto`**} *`port-list`*

- **`forceauth`** — Forces the specified wired authentication port(s) to *unconditionally authorize* all 802.1X authentication attempts, with an EAP success message.
- **`forceunauth`** — Forces the specified wired authentication port(s) to *unconditionally reject* all 802.1X authentication attempts with an EAP failure message.
- **`auto`** — Allows the specified wired authentication ports to process 802.1X authentication normally as determined for the user by the **set authentication dot1X** command.
- *`port-list`* — One or more wired authentication ports for which to set 802.1X port control.

Defaults — By default, wired authentication ports are set to **auto**.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command affects only wired authentication ports.

Examples — The following command forces port 1 to unconditionally accept all 802.1X authentication attempts:

```
WX4400# set dot1x port-control forceauth 1
success: authcontrol for 1 is set to FORCE-AUTH.
```

See Also

- **display port status** on page 73
- **display dot1x** on page 505

Downloaded from www.Manualslib.com manuals search engine

set dot1x quiet-period

Sets the number of seconds a WX remains quiet and does not respond to a supplicant after a failed authentication.

Syntax — **`set dot1x quiet-period`** *`seconds`*

- *`seconds`* — Specify a value between 0 and 65,535.

Defaults — The default is 60 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to set the quiet period to 90 seconds:

```
WX4400# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

See Also

- **clear dot1x quiet-period** on page 502
- **set dot1x wep-rekey-period** on page 518

set dot1x reauth

Determines whether the WX switch allows the reauthentication of supplicants (clients).

Syntax — **`set dot1x reauth`** {**`enable`** | **`disable`**}

- **`enable`** — Permits reauthentication.
- **`disable`** — Denies reauthentication.

Defaults — Reauthentication is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to enable reauthentication of supplicants (clients):

```
WX4400# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display dot1x** on page 505
- **set dot1x reauth-max** on page 514
- **set dot1x reauth-period** on page 515

---

set dot1x reauth-max

Sets the number of reauthentication attempts that the WX switch makes before the supplicant (client) becomes unauthorized.

Syntax — **`set dot1x reauth-max`** *`number-of-attempts`*

- *`number-of-attempts`* — Specify a value between 1 and 10.

Defaults — The default number of reauthentication attempts is 2.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

Examples — Type the following command to set the number of authentication attempts to 8:

```
WX4400# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

See Also

- **display dot1x** on page 505
- **clear dot1x reauth-max** on page 503

Downloaded from www.Manualslib.com manuals search engine

set dot1x reauth-period

Sets the number of seconds that must elapse before the WX switch attempts reauthentication.

Syntax — **`set dot1x reauth-period`** *`seconds`*

- *`seconds`* — Specify a value between 60 (1 minute) and 1,641,600 (19 days).

Defaults — The default is 3600 seconds (1 hour).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
WX4400# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

See Also

- **display dot1x** on page 505
- **clear dot1x reauth-period** on page 503

set dot1x timeout auth-server

Sets the number of seconds that must elapse before the WX switch times out a request to a RADIUS authentication server.

Syntax — **`set dot1x timeout auth-server`** *`seconds`*

- *`seconds`* — Specify a value between 1 and 65,535.

Defaults — The default is 30 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to set the authentication server timeout to 60 seconds:

```
WX4400# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **display dot1x** on page 505
- **clear dot1x timeout auth-server** on page 504

set dot1x timeout supplicant

Sets the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

Syntax — **set dot1x timeout supplicant** *seconds*

- *seconds* — Specify a value between 1 and 65,535.

Defaults — The default is 30 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to set the number of seconds for authentication session timeout to 300:

```
WX4400# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

See Also

- **display dot1x** on page 505
- **clear dot1x timeout auth-server** on page 504

set dot1x tx-period

Sets the number of seconds that must elapse before the WX switch retransmits an EAPoL packet.

Syntax — **set dot1x tx-period** *seconds*

- *seconds* — Specify a value between 1 and 65,535.

Defaults — The default is 5 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — Type the following command to set the number of seconds before the WX switch retransmits an EAPoL packet to 300:

```
WX4400# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

See Also

- **display dot1x** on page 505
- **clear dot1x tx-period** on page 505

set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

Syntax — **set dot1X wep-rekey** {**enable** | **disable**}

- **enable** — Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the **set dot1x wep-rekey-**period for each radio, associated VLAN, and encryption type. The WX generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages.
- **disable** — WEP broadcast and multicast keys are never rotated.

Defaults — WEP key rotation is enabled, by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Reauthentication is *not* required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

Examples — Type the following command to disable WEP key rotation:

```
WX4400# set dot1x wep-rekey disable
success: wep rekeying disabled
```

See Also

- **display dot1x** on page 505
- **set dot1x wep-rekey-period** on page 518

Downloaded from www.Manualslib.com manuals search engine

set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

Syntax — **`set dot1x wep-rekey-period`** *`seconds`*

- *`seconds`* — Specify a value between 30 and 1,641,600 (19 days).

Defaults — The default is 1800 seconds (30 minutes).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to set the WEP-rekey period to 300 seconds:

```
WX4400# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

See Also

- **display dot1x** on page 505
- **set dot1x wep-rekey** on page 517

Downloaded from www.Manualslib.com manuals search engine

18 SESSION MANAGEMENT COMMANDS

Use session management commands to display and clear administrative and network user sessions.

Commands by Usage

This chapter presents session management commands alphabetically. Use Table 88 to locate commands in this chapter based on their use.

Table 88 Session Management Commands by Usage

Type	Command
Administrative Sessions	**display sessions** on page 522
	clear sessions on page 519
Network Sessions	**display sessions network** on page 525
	clear sessions network on page 521

clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

Syntax — **`clear sessions`** {**`admin`** | **`console`** | **`telnet`** [**`client`** [*`session-id`*]]}

- **`admin`** — Clears sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- **`console`** — Clears sessions for all users with administrative access to the WX switch through a console plugged into the switch.
- **`telnet`** — Clears sessions for all users with administrative access to the WX switch through a Telnet connection.
- **`telnet client`** [*`session-id`*] — Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To clear all administrator sessions type the following command:

```
WX4400# clear sessions admin
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
WX4400# clear sessions console
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear all administrative Telnet sessions, type the following command:

```
WX4400# clear sessions telnet
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```
WX4400# clear sessions telnet client 0
```

See Also

- **display sessions** on page 522

Downloaded from www.Manualslib.com manuals search engine

clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

Syntax — **clear sessions network** {**user** *user-glob* | **mac-addr** *mac-addr-glob* | **vlan** *vlan-glob* | **session-id** *local-session-id*}

- **user** *user-glob* — Clears all network sessions for a single user or set of users.

  Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)

- **mac-addr** *mac-addr-glob* — Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)

- **vlan** *vlan-glob* — Clears all network sessions on a single VLAN or a set of VLANs.

  Specify a VLAN name, use the double-asterisk wildcard character (******) to specify all VLAN names, or use the single-asterisk wildcard character (*****) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 28.)

- **session-id** *local-session-id* — Clears the specified 802.1X network session. To find local session IDs, use the display sessions command.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The **clear sessions network** command clears network sessions by deauthenticating and, for wireless clients, disassociating them.

Downloaded from www.Manualslib.com manuals search engine

Examples — To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
WX4400# clear sessions network mac-addr 00:01:02:03:04:05
```

To clear session 9, type the following command:

```
WX1200# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

To clear the session of user *Natasha*, type the following command:

```
WX1200# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters *Jo*, type the following command:

```
WX1200# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN *red*, type the following command:

```
WX1200# clear sessions network vlan red
```

See Also

- **display sessions** on page 522
- **display sessions network** on page 525

display sessions

Displays session information and statistics for all users with administrative access to the WX switch, or for administrative users with either console or Telnet access.

Syntax — **display sessions** {**admin** | **console** | **telnet** [**client**]}

- **admin** — Displays sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- **console** — Displays sessions for all users with administrative access to the WX switch through a console plugged into the switch.

Downloaded from www.Manualslib.com manuals search engine

- **`telnet`** — Displays sessions for all users with administrative access to the WX switch through a Telnet connection.
- **`telnet client`** — Displays Telnet sessions from the CLI to remote devices.

Defaults — None.

Access — All, except for **display sessions telnet client**, which has enabled access.

History —Introduced in MSS Version 3.0.

Examples — To view information about sessions of administrative users, type the following command:

```
WX4400> display sessions admin
Tty         Username              Time (s)    Type
-------     --------------------  --------    ----
tty0                              3644        Console
tty2        tech                  6           Telnet
tty3        sshadmin              381         SSH

3 admin sessions
```

To view information about console users' sessions, type the following command:

```
WX4400> display sessions console
Tty         Username              Time (s)
-------     --------------------  --------
console                           8573
1 console session
```

To view information about Telnet users sessions, type the following command:

```
WX4400> display sessions telnet
Tty         Username              Time (s)
-------     --------------------  --------
tty2        sea                   7395
```

Downloaded from www.Manualslib.com manuals search engine

To view information about Telnet client sessions, type the following command:

```
wx4400# display sessions telnet client
Session   Server Address    Server Port    Client Port
-------   --------------    ------------   -----------
0          192.168.1.81     23             48000
1           10.10.1.22      23             48001
```

Table 89 describes the fields of the **display sessions admin**, **display sessions console**, and **display sessions telnet** displays.

Table 89 display sessions admin, display sessions console, and display sessions telnet Output

Field	Description
Tty	The Telnet terminal number, or *console* for administrative users connected through the console port.
Username	Up to 30 characters of the name of an authenticated user.
Time (s)	Number of seconds the session has been active.
Type	Type of administrative session: ▪ Console ▪ SSH ▪ Telnet

Table 90 describes the fields of the **display sessions telnet client** display.

Table 90 display sessions telnet client Output

Field	Description
Session	Session number assigned by MSS when the client session is established.
Server Address	IP address of the remote device.
Server Port	TCP port number of the remote device's TCP server.
Client Port	TCP port number MSS is using for the client side of the session.

See Also

- **clear sessions** on page 519

Downloaded from www.Manualslib.com manuals search engine

display sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax — **display sessions network**
[**user** *user-glob* | **mac-addr** *mac-addr-glob* | **ssid** *ssid-name* **vlan** *vlan-glob* | **session-id** *session-id* | **wired**] [**verbose**]

- **user** *user-glob* — Displays all network sessions for a single user or set of users.

  Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 26.)

- **mac-addr** *mac-addr-glob* — Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:).

  Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 27.)

- **ssid** *ssid-name* — Displays all network sessions for an SSID.

- **vlan** *vlan-glob* — Displays all network sessions on a single VLAN or a set of VLANs.

  Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 28.)

- **session-id** *local-session-id* — Displays the specified network session. To find local session IDs, use the **display sessions** command. The **verbose** option is not available with this form of the **display sessions network** command.

- **wired** — Displays all network sessions on wired authentication ports.

- **verbose** — Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.

Defaults — None.

Access — All.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 3.0. Output added to the **display network sessions verbose** command to indicate the user's authorization attributes and whether they were supplied through AAA or through configured SSID defaults in a service profile in MSS Version 4.1.

Usage — MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

- **Summary display** — See Table 91 on page 528.
- **Verbose display** — See Table 92 on page 529.
- **display sessions network session-id** display — See Table 93 on page 530.

Examples — To display summary information for all network sessions, type **display sessions network**. For example:

```
WX1200# display sessions network
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
EXAMPLE\Natasha                 4* 10.10.40.17        vlan-eng          3/1
host/laptop11.exmpl.com         6* 10.10.40.16        vlan-eng          3/2
nin@exmpl.com                 539* 10.10.40.17        vlan-eng          1/1
EXAMPLE\hosni                 302* 10.10.40.10        vlan-eng          3/1
                              563  00:0b:be:15:46:56  (none)            1/2
jose@exmpl.com                380* 10.30.40.8         vlan-eng          1/1
00:30:65:16:8d:69             443* 10.10.40.19        vlan-wep          3/1
EXAMPLE\Geetha                459* 10.10.40.18        vlan-eng          3/2
8 sessions total
```

The following command displays summary information about the sessions for MAC address 00:05:5d:7e:98:1a:

```
WX1200# display sessions network mac-addr 00:05:5d:7e:98:1a
User                        Sess  IP or MAC       VLAN         Port/
Name                          ID  Address         Name         Radio
--------------------------- ----  --------------- ------------ -----
EXAMPLE\Havel                 13* 10.10.10.40     vlan-eng      1/2
```

The following command displays summary information about all the sessions of users whose names begin with *E*:

```
WX1200# display sessions network user E*
User                        Sess  IP or MAC       VLAN         Port/
Name                          ID  Address         Name         Radio
--------------------------- ----  --------------- ------------ -----
```

Downloaded from www.Manualslib.com manuals search engine

```
EXAMPLE\Singh                12* 10.10.10.30     vlan-eng      3/2
EXAMPLE\Havel                13* 10.10.10.40     vlan-eng      1/2
2 sessions match criteria (of 3 total)
```

(Table 91 on page 528 describes the summary displays of **display sessions network** commands.)

The following command displays detailed (verbose) session information about user nin@example.com:

```
WX1200# display sessions network user nin@example.com verbose
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
nin@example.com                5* 10.20.30.40       vlan-eng         1/1
Client MAC: 00:02:2d:6e:ab:a5   GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE                  (prev AUTHORIZED)
now on: WX 192.168.12.7, AP/radio  1/1, AP 00:0b:0e:00:05:fe, as of 00:23:32 ago
1 sessions match criteria (of 10 total)
```

The following command displays verbose output about the sessions of all current network users:

```
WX1200# display sessions network verbose
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
SHUTTLE2\exmpl                 6* 10.3.8.55         default          3/1
Client MAC: 00:06:25:13:08:33   GID: SESS-4-000404-98441-c807c14b
State: ACTIVE                  (prev AUTHORIZED)
now on: WX 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:00:24 ago
  from: WX 10.3.8.103, AP/radio  6/1, AP 00:0b:0e:00:05:d7, as of
00:01:07 ago
  from: WX 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:01:53 ago

Vlan-Name=default (service-profile)
Service-Type=2 (service-profile)
End-Date=52/06/07-08:57 (AAA)
Start-Date=05/04/11-10:00 (AAA)


1 sessions total
```

Downloaded from www.Manualslib.com manuals search engine

(Table 92 on page 529 describes the additional fields of the **verbose** output of **display sessions network** commands.)

The following command displays information about network session 27:

```
WX1200# display sessions network session-id 27
Global Id: SESS-27-000430-835586-58dfe5a
State: ACTIVE
Port/Radio: 3/1
MAC Address: 00:00:2d:6f:44:77
User Name: EXAMPLE Natasha
IP Address: 10.10.40.17
Vlan Name: vlan-eng
Tag: 1
Session Timeout: 1800
Authentication Method: PEAP, using server 10.10.70.20
Session statistics as updated from AP:
Unicast packets in: 653
Unicast bytes in: 46211
Unicast packets out: 450
Unicast bytes out: 50478
Multicast packets in: 317
Multicast bytes in: 10144
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 2
Last packet signal strength: -67 dBm
Last packet data S/N ratio: 55
```

Table 91 describes the output of this command. For descriptions of the fields of **display sessions network session-id** output, see Table 93 on page 530.

Table 91 display sessions network (summary) Output

Field	Description
User Name	Up to 30 characters of the name of the authenticated user of this session.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to the session ID indicates fully active sessions.
IP or MAC Address	IP address of the session user, or the user's MAC address if the user has not yet received an IP address.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the user is accessing this session.

Downloaded from www.Manualslib.com manuals search engine

Table 92 Additional display sessions network verbose Output

Field	Description
Client MAC	MAC address of the session user.
GID	Global session ID, a unique session number within a Mobility Domain.
State	Status of the session: ▪ **AUTH, ASSOC REQ** — Client is being associated by the 802.1X protocol. ▪ **AUTH AND ASSOC** — Client is being associated by the 802.1X protocol, and the user is being authenticated. ▪ **AUTHORIZING** — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. ▪ **AUTHORIZED** — User has been authorized by an AAA method. ▪ **ACTIVE** — User's AAA attributes have been applied, and the user is active on the network. ▪ **DEASSOCIATED** — One of the following: Wireless client has sent the WX switch a disassociate message. User associated with one of the current WX switch's MAP access points has appeared at another WX switch in the Mobility Domain. ▪ **ROAMING AWAY** — The W switch has been sent a request to transfer the user, who is roaming, to another WX switch. ▪ **STATUS UPDATED** — WX switch is receiving a final update from a MAP access point about the user, who has roamed away. ▪ **WEB_AUTHING** — User is being authenticated by WebAAA. ▪ **WIRED AUTH'ING** — User is being authenticated by the 802.1X protocol on a wired authentication port. ▪ **KILLING** — User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event.
now on	IP address and port and radio numbers of the session's current WX switch, the MAC address of the MAP access point, and the last update time.
from	IP address and port and radio numbers of the session's previous WX switch, the MAC address of the MAP access point, and the last update time. Up to six roaming events are tracked in this display.
Vlan-Name Service-Type End-Date Start-Date	Authorization attributes for the user and how they were assigned. The authorization attributes can be assigned either by a RADIUS server or the local database (indicated in the output by AAA), or by SSID default settings in the service profile the user used to gain access to the network (indicated in the output by service-profile).

Downloaded from www.Manualslib.com manuals search engine

Table 93 display sessions network session-id Output

Field	Description
Global Id	A unique session identifier within the Mobility Domain.
State	Status of the session: ▪ **AUTH, ASSOC REQ** — Client is being associated by the 802.1X protocol. ▪ **AUTH AND ASSOC** — Client is being associated by the 802.1X protocol, and the user is being authenticated. ▪ **AUTHORIZING** — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. ▪ **AUTHORIZED** — User has been authorized by an AAA method. ▪ **ACTIVE** — User's AAA attributes have been applied, and the user is active on the network. ▪ **DEASSOCIATED** — One of the following: Wireless client has sent the WX switch a disassociate message. User associated with one of the current WX switch's MAP access points has appeared at another WX switch in the Mobility Domain. ▪ **ROAMING AWAY** — The WX switch has been sent a request to transfer the user, who is roaming, to another WX switch. ▪ **STATUS UPDATED** — WX switch is receiving a final update from an MAP access point about the user, who has roamed away. ▪ **WEB_AUTHING** — User is being authenticated by WebAAA. ▪ **WIRED AUTH'ING** — User is being authenticated by the 802.1X protocol on a wired authentication port. ▪ **KILLING** — User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event.
Port/Radio	Number of the port and radio through which the user is accessing this session.
MAC address	MAC address of the session user.
User Name	Name of the authenticated user of this session
IP Address	IP address of the session user.
Vlan Name	Name of the VLAN associated with the session.
Tag	System-wide supported VLAN tag type.

Downloaded from www.Manualslib.com manuals search engine

Table 93 display sessions network session-id Output (continued)

Field	Description
Session Timeout	Assigned session timeout in seconds.
Authentication Method	Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server.
Session statistics as updated from AP	Time the session statistics were last updated from the MAP access point, in seconds since a fixed standard date and time.
Unicast packets in	Total number of unicast packets received from the user by the WX (64-bit counter).
Unicast bytes in	Total number of unicast bytes received from the user by the WX (64-bit counter).
Unicast packets out	Total number of unicast packets sent by the WX to the user (64-bit counter).
Unicast bytes out	Total number of unicast bytes sent by the WX to the user (64-bit counter).
Multicast packets in	Total number of multicast packets received from the user by the WX (64-bit counter).
Multicast bytes in	Total number of multicast bytes received from the user by the WX (64-bit counter).
Number of packets with encryption errors	Total number of decryption failures.
Number of bytes with encryption errors	Total number of bytes with decryption errors.
Last packet data rate	Data transmit rate, in megabits per second (Mbps), of the last packet received by the MAP access point.
Last packet signal strength	Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the MAP access point.
Last packet data S/N ratio	Signal-to-noise ratio of the last packet received by the MAP access point.

See Also

- **clear sessions network** on page 521

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

19 RF DETECTION COMMANDS

MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a 3Com switch and is not a member of the ignore list configured on the seed switch of the Mobility Domain. The ignore list is a list of third-party (*friendly*) BSSIDs that are not rogues.

MSS can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters only on the seed switch of a Mobility Domain.

Commands by Usage

This chapter presents RF detection commands alphabetically. Use Table 94 to locate the commands in this chapter based on their use.

Table 94 RF Detection Commands by Usage

Type	Command
Rogue Information	**display rfdetect clients** on page 539
	display rfdetect mobility-domain on page 546
	display rfdetect data on page 544
	display rfdetect visible on page 552
	display rfdetect counters on page 542
Countermeasures	**display rfdetect countermeasures** on page 541
Permitted Vendor List	**set rfdetect vendor-list** on page 561

Downloaded from www.Manualslib.com manuals search engine

Table 94 RF Detection Commands by Usage (continued)

Type	Command
	display rfdetect vendor-list on page 551
	clear rfdetect vendor-list on page 537
Permitted SSID List	**set rfdetect ssid-list** on page 560
	display rfdetect ssid-list on page 550
	clear rfdetect ssid-list on page 536
Client Black List	**set rfdetect black-list** on page 555
	display rfdetect black-list on page 538
	clear rfdetect black-list on page 535
Attack List	**set rfdetect attack-list** on page 554
	display rfdetect attack-list on page 537
	clear rfdetect attack-list on page 534
Ignore List	**set rfdetect ignore** on page 558
	display rfdetect ignore on page 546
	clear rfdetect ignore on page 535
MAP Signatures	**set rfdetect signature** on page 560
Log Messages	**set rfdetect log** on page 559

clear rfdetect attack-list

Removes a MAC address from the attack list.

Syntax — **`clear rfdetect attack-list`** *`mac-addr`*

- *`mac-addr`* — MAC address you want to remove from the attack list.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
wx4400# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear rfdetect attack-list** on page 534
- **display rfdetect attack-list** on page 537

clear rfdetect black-list

Removes a MAC address from the client black list.

Syntax — **`clear rfdetect black-list`** *`mac-addr`*

- *`mac-addr`* — MAC address you want to remove from the black list.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command removes MAC address 11:22:33:44:55:66 from the black list:

```
WX1200# clear rfdetect black-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer blacklisted.
```

See Also

- **set rfdetect black-list** on page 555
- **display rfdetect black-list** on page 538

clear rfdetect ignore

Removes a device from the ignore list for RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — **`clear rfdetect ignore`** *`mac-addr`*

- *`mac-addr`* — Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the ignore list.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command removes BSSID *aa:bb:cc:11:22:33* from the ignore list for RF scans:

```
WX1200# clear rfdetect ignore aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer ignored.
```

See Also

- **display rfdetect ignore** on page 546
- **set rfdetect ignore** on page 558

clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

Syntax — **clear rfdetect ssid-list** *ssid-name*

- *ssid-name* — SSID name you want to remove from the permitted SSID list.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command clears SSID *mycorp* from the permitted SSID list:

```
WX1200# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

See Also

- **set rfdetect ssid-list** on page 560
- **display rfdetect ssid-list** on page 550

Downloaded from www.Manualslib.com manuals search engine

clear rfdetect vendor-list

Removes an entry from the permitted vendor list.

Syntax — **`clear rfdetect vendor-list {client | ap}`** *`mac-addr`* **`| all`**

- **`client | ap`** — Specifies whether the entry is for an AP brand or a client brand.
- *`mac-addr`* **`| all`** — Organizationally Unique Identifier (OUI) to remove.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
WX4400# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client
vendor-list.
```

See Also

- **set rfdetect vendor-list** on page 561
- **display rfdetect vendor-list** on page 551

display rfdetect attack-list

Displays information about the MAC addresses in the attack list.

Syntax — **`display rfdetect attack-list`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example shows the attack list on WX switch:

```
WX1200# display rfdetect attack-list
Total number of entries: 1
 Attacklist MAC    Port/Radio/Chan   RSSI      SSID
----------------- ----------------- ------ ------------
11:22:33:44:55:66  dap 2/1/11       -53    rogue-ssid
```

See Also

- **clear rfdetect attack-list** on page 534
- **set rfdetect attack-list** on page 554

display rfdetect black-list

Displays information abut the clients in the client black list.

Syntax — **display rfdetect black-list**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following example shows the client black list on WX switch:

```
WX1200# display rfdetect black-list
Total number of entries: 1
  Blacklist MAC         Type          Port   TTL
----------------- ----------------- ------- ---
11:22:33:44:55:66 configured        -         -
11:23:34:45:56:67 assoc req flood   3        25
```

See Also

- **clear rfdetect black-list** on page 535
- **set rfdetect black-list** on page 555

Downloaded from www.Manualslib.com manuals search engine

display rfdetect clients

Displays the wireless clients detected by a WX switch.

Syntax — **`display rfdetect clients [mac`** *`mac-addr`***`]`**

`mac` *`mac-addr`* — Displays detailed information for a specific client.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command shows information about all wireless clients detected by a WX switch's MAPs:

```
WX4400# display rfdetect clients
Total number of entries: 30
Client MAC        Client       AP MAC          AP    Port/Radio    NoL Type  Last
                  Vendor                     Vendor      /Channel            seen
----------------- ------- ----------------- ------- ------------- --- ----- ----

00:03:7f:bf:16:70 Unknown           Unknown           dap 1/1/6     1 intfr 207
00:04:23:77:e6:e5   Intel           Unknown           dap 1/1/2     1 intfr 155
00:05:5d:79:ce:0f  D-Link           Unknown           dap 1/1/149   1 intfr 87
00:05:5d:7e:96:a7  D-Link           Unknown           dap 1/1/149   1 intfr 117
00:05:5d:7e:96:ce  D-Link           Unknown           dap 1/1/157   1 intfr 162
00:05:5d:84:d1:c5  D-Link           Unknown           dap 1/1/1     1 intfr 52
```

The following command displays more details about a specific client:

```
WX4400# display rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
    Port: dap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago):
84
    Bssid: 00:0b:0e:01:02:00, Vendor: 3Com, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
    Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Table 95 and Table 96 describe the fields in these displays.

Downloaded from www.Manualslib.com manuals search engine

Table 95 display rfdetect clients Output

Field	Description
Client MAC	MAC address of the client.
Client Vendor	Company that manufactures or sells the client.
AP MAC	MAC address of the radio with which the rogue client is associated.
AP Vendor	Company that manufactures or sells the AP with which the rogue client is associated.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed MAP, the connection number is labeled *dap*. (This stands for *distributed ap*.)
NoL	Number of listeners. This is the number of MAP radios that detected the rogue client.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Last seen	Number of seconds since a MAP radio last detected 802.11 packets from the device.

Table 96 display rfdetect clients mac Output

Field	Description
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Rate	The data rate of the client.
Last Seen	Number of seconds since a MAP radio last detected 802.11 packets from the device.
BSSID	MAC address of the SSID with which the rogue client is associated.
Vendor	Company that manufactures or sells the AP with which the rogue client is associated.

Downloaded from www.Manualslib.com manuals search engine

Table 96 display rfdetect clients mac Output (continued)

Field	Description
Typ	Classification of the rogue device: ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Dst	MAC addressed to which the last 802.11 packet detected from the client was addressed.
Last Rogue Status Check	Number of seconds since the WX switch looked on the air for the AP with which the rogue client is associated. The switch looks for the client's AP by sending a packet from the wired side of the network addressed to the client, and watching the air for a wireless packet containing the client's MAC address.

display rfdetect countermeasures

Displays the current status of countermeasures against rogues in the Mobility Domain.

Syntax — **`display rfdetect countermeasures`**

Defaults — None.

Access — Enabled.

History —Output no longer lists rogues for which countermeasures have not been started in MSS Version 4.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

Examples — The following example displays countermeasures status for the Mobility Domain:

```
WX4400# display rfdetect countermeasures
Total number of entries: 190
Rogue MAC         Type  Countermeasures    WX-IPaddr       Port/Radio
                        Radio Mac                             /Channel
----------------- ----- ------------------ --------------- -------------
00:0b:0e:00:71:c0 intfr  00:0b:0e:44:55:66 10.1.1.23       dap 4/1/6
00:0b:0e:03:00:80 rogue  00:0b:0e:11:22:33 10.1.1.23       dap 2/1/11
```

Downloaded from www.Manualslib.com manuals search engine

Table 97 describes the fields in this display.

Table 97 display rfdetect countermeasures Output

Field	Description
Rogue MAC	BSSID of the rogue.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Countermeasures Radio MAC	MAC address of the 3Com radio sending countermeasures against the rogue.
WX-IPaddr	System IP address of the WX switch that is managing the MAP that is sending or will send countermeasures.
Port/Radio/Channel	Port number, radio number, and channel number of the countermeasures radio. For a Distributed MAP, the connection number is labeled *dap*. (This stands for *distributed ap*.)

See Also

- **set radio-profile countermeasures** on page 355

display rfdetect counters

Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the MAPs managed by a WX switch.

Syntax — **`display rfdetect counters`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows counters for rogue activity detected by a WX switch:

```
WX4400# display rfdetect counters
Type                                                Current      Total
--------------------------------------------------- ------------ ------------

Rogue access points                                           0            0
Interfering access points                                   139         1116
Rogue 802.11 clients                                          0            0
Interfering 802.11 clients                                    4          347
802.11 adhoc clients                                          0            1
Unknown 802.11 clients                                       20          965
Interfering 802.11 clients seen on wired network              0            0
802.11 probe request flood                                    0            0
802.11 authentication flood                                   0            0
802.11 null data flood                                        0            0
802.11 mgmt type 6 flood                                      0            0
802.11 mgmt type 7 flood                                      0            0
802.11 mgmt type d flood                                      0            0
802.11 mgmt type e flood                                      0            0
802.11 mgmt type f flood                                      0            0
802.11 association flood                                      0            0
802.11 reassociation flood                                    0            0
802.11 disassociation flood                                   0            0
Weak wep initialization vectors                               0            0
Spoofed access point mac-address attacks                      0            0
Spoofed client mac-address attacks                            0            0
Ssid masquerade attacks                                       1           12
Spoofed deauthentication attacks                              0            0
Spoofed disassociation attacks                                0            0
Null probe responses                                        626        11380
Broadcast deauthentications                                   0            0
FakeAP ssid attacks                                           0            0
FakeAP bssid attacks                                          0            0
Netstumbler clients                                           0            0
Wellenreiter clients                                          0            0
Active scans                                               1796         4383
Wireless bridge frames                                      196          196
Adhoc client frames                                           8            0
Access points present in attack-list                          0            0
Access points not present in ssid-list                        0            0
Access points not present in vendor-list                      0            0
Clients not present in vendor-list                            0            0
Clients added to automatic black-list                         0            0
```

Downloaded from www.Manualslib.com manuals search engine

display rfdetect data

Displays all the BSSIDs detected by an individual WX switch during an RF detection scan. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

Syntax — **`display rfdetect data`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Vendor, Type, and Flag fields added in MSS Version 4.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The output applies only to the switch on which you enter the command. To display all devices that a specific 3Com radio has detected, even if the radio is managed by another WX switch, use the **display rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **display rfdetect mobility-domain** command on the seed switch.

Only one MAC address is listed for each 3Com radio, even if the radio is beaconing multiple SSIDs.

Examples — The following command shows the devices detected by this WX switch during the most recent RF detection scan:

```
WX1200# display rfdetect data
Total number of entries: 7
          BSSID        Port/Rad   Chan   RSSI Age SSID
    ----------------  --------  ------  ---- --- --------
    00:06:25:09:39:4a     5/1        3  0     15 rack29-hostap
    00:06:25:51:e9:ff     4/1       10  -85   15 Arrow
    00:06:25:51:e9:ff     5/1       10  -84   15 Arrow
    00:0b:0e:00:00:00     4/1        1  -78   15 gary-eng
    00:0b:0e:00:02:00     4/1       11  -76   15 public
    00:0b:0e:00:02:00     5/1       11  -74   15 public
    00:0b:0e:00:02:01     4/1       56  -68   15 public
```

Table 98 describes the fields in this display.

Downloaded from www.Manualslib.com manuals search engine

Table 98 display rfdetect data Output

Field	Description
BSSID	BSSID detected by a MAP radio on this WX switch.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch's FDB and is therefore on the network. ▪ intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch's FDB and is not actually on the network, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed MAP, the connection number is labeled *dap*. (This stands for *distributed ap*.).
Flags	Classification and encryption information for the rogue: ▪ The i, a, or u flag indicates the classification. ▪ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
RSSI	Received signal strength indication (RSSI) — the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Age	Age of the rogue listing, in seconds. Rogues age out of the rogue list after one minute.
SSID	Service set identifier (SSID) associated with the BSSID.

See Also

- **display rfdetect mobility-domain** on page 546
- **display rfdetect visible** on page 552

Downloaded from www.Manualslib.com manuals search engine

display rfdetect ignore

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — **`display rfdetect ignore`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following example displays the list of ignored devices:

```
WX4400# display rfdetect ignore
Total number of entries: 2
   Ignore MAC
-----------------
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

See Also

- **clear rfdetect ignore** on page 535
- **set rfdetect ignore** on page 558

display rfdetect mobility-domain

Displays the rogues detected by all WX switches in the Mobility Domain during RF detection scans.

Syntax — **`display rfdetect mobility-domain`**
`[ssid` *`ssid-name`* **`| bssid`** *`mac-addr`***`]`**

- **`ssid`** *`ssid-name`* — Displays rogues that are using the specified SSID.
- **`bssid`** *`mac-addr`* — Displays rogues that are using the specified BSSID.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. **Bssid** and **ssid** options added; Vendor, Type and Flag fields added in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — This command is valid only on the seed switch of the Mobility Domain. To display rogue information for an individual switch, use the **display rfdetect data** command on that switch.

Only rogues are listed. To display all devices detected, including 3Com radios, use the **display rfdetect data** command.

Examples — The following example displays information about the BSSIDs detected in the Mobility Domain managed by the seed switch:

```
WX1200# display rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor       Type  Flags  SSID
----------------- ------------ ----- ------ --------------------------------
00:07:50:d5:cc:91        Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78        Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54        Cisco intfr i-----
00:0a:5e:4b:4a:c0         3Com intfr i----- public
00:0a:5e:4b:4a:c2         3Com intfr i----w 3Comwlan
00:0a:5e:4b:4a:c4         3Com intfr ic---- 3Com-ccmp
00:0a:5e:4b:4a:c6         3Com intfr i----w 3Com-tkip
00:0a:5e:4b:4a:c8         3Com intfr i----w 3Com-voip
00:0a:5e:4b:4a:ca         3Com intfr i----- 3Com-webaaa
...
```

The lines in this display are compiled from data from multiple listeners (MAP radios). If an item has the value *unresolved*, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when a MAP or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID *3com-webaaa*.

```
WX1200# display rfdetect mobility-domain ssid 3Com-webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID: 3Com-webaaa
Type: intfr Adhoc: no Crypto-types: clear

  WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/11 Mac:
00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -85 SSID: 3Com-webaaa
```

Downloaded from www.Manualslib.com manuals search engine

```
BSSID: 00:0b:0e:00:7a:8a Vendor: 3Com SSID: 3com-webaaa
Type: intfr Adhoc: no Crypto-types: clear

  WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/1 Mac:
00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -75 SSID: 3Com-webaaa

  WX-IPaddress: 10.3.8.103 Port/Radio/Ch: dap 1/1/1 Mac:
00:0b:0e:76:56:82
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -76 SSID: 3Com-webaaa
```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (MAP radios) that detected the SSID. Each set of indented lines is for a separate MAP listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information is shown for each of the BSSIDs, and information about the listeners for each BSSID are shown.

The following command displays detailed information for a BSSID.

```
WX1200# display rfdetect mobility-domain bssid
00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

  WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/2/56 Mac:
00:0b:0e:00:0a:6b
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp

  WX-IPaddress: 10.3.8.103 Port/Radio/Ch: dap 1/1/157 Mac:
00:0b:0e:76:56:82
  Device-type: rogue Adhoc: no Crypto-types: clear
  RSSI: -72 SSID: notmycorp
```

Table 99 and Table 100 describe the fields in these displays.

Downloaded from www.Manualslib.com manuals search engine

Table 99 display rfdetect mobility-domain Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch's FDB and is therefore on the network. ▪ intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch's FDB and is not actually on the network, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Flags	Classification and encryption information for the rogue: ▪ The i, a, or u flag indicates the classification. ▪ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

Table 100 display rfdetect mobility-domain ssid or bssid Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
SSID	SSID used by the detected device.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Adhoc	Indicates whether the rogue is an infrastructure rogue (is using an AP) or is operating in ad-hoc mode.

Downloaded from www.Manualslib.com manuals search engine

Table 100 display rfdetect mobility-domain ssid or bssid Output (continued)

Field	Description
Crypto-Types	Encryption type: clear (no encryption) ccmp tkip wep104 (WPA 104-bit WEP) wep40 (WPA 40-bit WEP) wep (non-WPA WEP)
WX-IPaddress	System IP address of the WX switch that detected the rogue.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed MAP, the connection number is labeled *dap*. (This stands for *distributed ap*.)
Mac	MAC address of the radio that detected the rogue.
Device-type	Device type detected by the MAP radio.
Adhoc	Ad-hoc status (yes or no) detected by the MAP radio.
Crypto-Types	Encryption type detected by the MAP radio.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
SSID	SSID mapped to the BSSID.

See Also

- **display rfdetect data** on page 544
- **display rfdetect visible** on page 552

display rfdetect ssid-list

Displays the entries in the permitted SSID list.

Syntax — **`display rfdetect ssid-list`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following example shows the permitted SSID list on WX switch:

```
WX4400# display rfdetect ssid-list
Total number of entries: 3
       SSID
-----------------
           mycorp
         corporate
             guest
```

See Also

- **clear rfdetect ssid-list** on page 536
- **set rfdetect ssid-list** on page 560

display rfdetect vendor-list

Displays the entries in the permitted vendor list.

Syntax — **display rfdetect vendor-list**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following example shows the permitted vendor list on WX switch:

```
WX1200# display rfdetect vendor-list
Total number of entries: 1
       OUI         Type
----------------- ------
aa:bb:cc:00:00:00 client
11:22:33:00:00:00 ap
```

See Also

- **clear rfdetect vendor-list** on page 537
- **set rfdetect vendor-list** on page 561

Downloaded from www.Manualslib.com manuals search engine

display rfdetect visible

Displays the BSSIDs discovered by a specific 3Com radio. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

Syntax — **display rfdetect visible** *mac-addr*

Syntax — **display rfdetect visible ap** *map-num* [**radio** {**1** | **2**}]

Syntax — **display rfdetect visible dap** *dap-num* [**radio** {**1** | **2**}]

- *mac-addr* — Base MAC address of the 3Com radio.

  To display the base MAC address of a 3Com radio, use the **display {ap | dap} status** command.
- *map-num* — Port connected to the MAP access point for which to display neighboring BSSIDs.
- *dap-num* — Number of a Distributed MAP for which to display neighboring BSSIDs.
- **radio 1** — Shows neighbor information for radio 1.
- **radio 2** — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If a 3Com radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the **display rfdetect mobility-domain** command on the seed switch.

Examples — The following command displays the devices detected by 3Com radio 00:0b:0e:00:0a:6a:

```
WX1200# display rfdetect visible 00:0b:0e:00:0a:6a ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI Flags  SSID
```

Downloaded from www.Manualslib.com manuals search engine

```
----------------- ------- ----- --- ---- ------ ------------------------------
00:07:50:d5:cc:91   Cisco intfr   6  -60 i----w r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr   6  -82 i----w r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr   2  -54 i-----
00:0a:5e:4b:4a:c0    3Com intfr  11  -57 i----- public
00:0a:5e:4b:4a:c2    3Com intfr  11  -86 i-t1-- 3Comwlan
00:0a:5e:4b:4a:c4    3Com intfr  11  -85 ic---- 3com-ccmp
00:0a:5e:4b:4a:c6    3Com intfr  11  -85 i-t--- 3com-tkip
00:0a:5e:4b:4a:c8    3Com intfr  11  -83 i----w 3com-voip
00:0a:5e:4b:4a:ca    3Com intfr  11  -85 i----- 3com-webaaa
...
```

Table 101 describes the fields in this display.

Table 101 display rfdetect visible Output

Field	Description
Transmit MAC	MAC address the rogue device that sent the 802.11 packet detected by the MAP radio.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Ch	Channel number on which the radio detected the rogue.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Flags	Classification and encryption information for the rogue: ▪ The i, a, or u flag indicates the classification. ▪ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

See Also

- **display rfdetect data** on page 544
- **display rfdetect mobility-domain** on page 546

Downloaded from www.Manualslib.com manuals search engine

set rfdetect active-scan

Disables or reenables active RF detection scanning on a WX switch. When active scanning is enabled, the MAP radios managed by the switch look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Syntax — **`set rfdetect active-scan`** {**`enable`** | **`disable`**}

- **`enable`** — Enables active RF detection scanning.
- **`disable`** — Disables active RF detection scanning.

Defaults — Active scanning is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The command takes effect only on that switch.

Examples — The following command disables active scanning on a WX switch:

```
WX1200# set rfdetect active-scan disable
success:  off-channel scanning is disabled.
```

set rfdetect attack-list

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

Syntax — **`set rfdetect attack-list`** *`mac-addr`*

- *`mac-addr`* — MAC address you want to attack.

Defaults — The attack list is empty by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The attack list applies only to the WX switch on which the list is configured. WX switches do not share attack lists.

Downloaded from www.Manualslib.com manuals search engine

When on-demand countermeasures are enabled (with the **set radio-profile countermeasures configured** command) only those devices configured in the attack list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

Examples — The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
WX4400# set rfdetect attack-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now in attacklist.
```

See Also

- **clear rfdetect attack-list** on page 534
- **display rfdetect attack-list** on page 537
- **set radio-profile countermeasures** on page 355

set rfdetect black-list

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. MSS drops all packets from the clients on the black list.

Syntax — **set rfdetect black-list** *mac-addr*

- *mac-addr* — MAC address you want to place on the black list.

Defaults — The client black list is empty by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — In addition to manually configured entries, the list can contain entries added by MSS. MSS can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the WX switch on which the list is configured. WX switches do not share client black lists.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
WX1200# set rfdetect black-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now blacklisted.
```

See Also

- **set rfdetect black-list** on page 555
- **display rfdetect black-list** on page 538

set rf detect countermeasures

Enables or disables countermeasures for the Mobility Domain. Countermeasures are packets sent by a radio to prevent clients from being able to use a rogue access point.

CAUTION: *Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.*

Syntax — **set rfdetect countermeasures** {**enable** | **disable**}

- **enable** — Enables countermeasures.
- **disable** — Disables countermeasures.

Defaults — Countermeasures are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

Examples — The following command enables countermeasures for the Mobility Domain managed by this seed switch:

```
WX1200# set rfdetect countermeasures enable
success:  countermeasures are now enabled.
```

See Also

- **clear rfdetect attack-list** on page 534
- **display rfdetect ignore** on page 546
- **set rfdetect countermeasures mac** on page 557

Downloaded from www.Manualslib.com manuals search engine

set rfdetect countermeasures mac

Starts countermeasures against a specific rogue.

Syntax — **`set rfdetect countermeasures mac`** *`mac-addr`*

- *`mac-addr`* — Basic service set identifier (BSSID) of the rogue. Enter the BSSID in MAC address format, using a colon between each octet (for example: aa:bb:cc:dd:ee:ff).

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Use this command to immediately begin countermeasures against a specific rogue in the rogue list. The MAC address you specify must be in the list of rogues generated by RF detection scans. MSS can issue countermeasures only against a device that is in the rogue list.

You can start countermeasures against more than one BSSID by typing additional **set rfdetect countermeasures mac** commands.

*After you type the first **set rfdetect countermeasures mac** command, MSS does not issue countermeasures against any devices except the ones you specify using this command. To resume normal countermeasures operation, where MSS automatically issues countermeasures against detected rogues, use the **clear rfdetect countermeasures mac all** command.*

This command is valid only on the seed switch of the Mobility Domain. The countermeasures take effect only if countermeasures are enabled for the Mobility Domain, using the **set rfdetect countermeasures enable** command.

This command does not become part of the configuration file when you save the configuration and therefore is not reloaded if the switch is restarted.

Examples — The following command begins countermeasures against rogue BSSID aa:bb:cc:11:22:33:

```
WX1200# set rfdetect countermeasures mac aa:bb:cc:11:22:33
success:  set rfdetect countermeasures mac aa:bb:cc:11:22:33
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear rfdetect attack-list** on page 534
- **display rfdetect ignore** on page 546
- **set rf detect countermeasures** on page 556

set rfdetect ignore

Configures a list of known devices to ignore during an RF scan. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — **`set rfdetect ignore`** *`mac-addr`*

- *`mac-addr`* — BSSID (MAC address) of the device to ignore.

Defaults — MSS reports all unknown BSSIDs detected during an RF scan.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Use this command to identify third-party APs and other devices you are already aware of and do not want MSS to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and MSS does not issue the countermeasures. Countermeasures apply only to rogue devices.

If you add a device that MSS has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

After you add a device that has been classified as a rogue to the ignore list, the device remains classified as a rogue for at least 10 minutes. After 10 minutes, MSS reclassifies the device as an interfering device.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command configures MSS to ignore BSSID *aa:bb:cc:11:22:33* during RF scans:

```
WX1200# set rfdetect ignore aa:bb:cc:11:22:33
success:  MAC aa:bb:cc:11:22:33 is now ignored.
```

See Also

- **clear rfdetect ignore** on page 535
- **display rfdetect ignore** on page 546

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax — **set rfdetect log** {**enable** | **disable**}

- **enable** — Enables logging of rogues.
- **disable** — Disables logging of rogues.

Defaults — RF detection logging is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the **display log buffer** command to display the messages in the seed switch's log message buffer.

Examples — The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
WX1200# set rfdetect log enable
success:  rfdetect logging is enabled.
```

See Also

- **display log buffer** on page 610

Downloaded from www.Manualslib.com manuals search engine

set rfdetect signature

Enables MAP signatures. A MAP signature is a set of bits in a management frame sent by a MAP that identifies that MAP to MSS. If someone attempts to spoof management packets from a 3Com MAP, MSS can detect the spoof attempt.

Syntax — **`set rfdetect signature {enable | disable}`**

- **`enable`** — Enables MAP signatures.
- **`disable`** — Disables MAP signatures.

Defaults — MAP signatures are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The command applies only to MAPs managed by the WX switch on which you enter the command. To enable signatures on all MAPs in a Mobility Domain, enter the command on each WX switch in the Mobility Domain.

You must use the same MAP signature setting (enabled or disabled) on all WX switches in a Mobility Domain.

Examples — The following command enables MAP signatures on a WX switch:

```
WX1200# set rfdetect signature enable
success:  signature is now enabled.
```

set rfdetect ssid-list

Adds an SSID to the permitted SSID list.The permitted SSID list specifies the SSIDs that are allowed on the network. If MSS detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

Syntax — **`set rfdetect ssid-list`** *`ssid-name`*

- *`ssid-name`* — SSID name you want to add to the permitted SSID list.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, MSS allows traffic only for the SSIDs that are on the list.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The permitted SSID list applies only to the WX switch on which the list is configured. WX switches do not share permitted SSID lists.

If you add a device that MSS has classified as a rogue to the permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted SSID list merely indicates that the device is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples — The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
WX1200# set rfdetect ssid-list mycorp
success:  ssid mycorp is now in ssid-list.
```

See Also

- **clear rfdetect ssid-list** on page 536
- **display rfdetect ssid-list** on page 550

set rfdetect vendor-list

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. MSS does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

Syntax — **`set rfdetect vendor-list {client | ap}`** *`mac-addr`*

- **`client | ap`** — Specifies whether the entry is for an AP brand or a client brand.
- *`mac-addr`* — Organizationally Unique Identifier (OUI) to remove.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, MSS allows only the devices whose OUIs are on the list.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The permitted vendor list applies only to the WX switch on which the list is configured. WX switches do not share permitted vendor lists.

If you add a device that MSS has classified as a rogue to the permitted vendor list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list merely indicates that the device is from an allowed vendor. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples — The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
WX1200# set rfdetect vendor-list client aa:bb:cc:00:00:00
success:  MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

See Also

- **clear rfdetect vendor-list** on page 537
- **display rfdetect vendor-list** on page 551

Downloaded from www.Manualslib.com manuals search engine

20 File Management Commands

Use file management commands to manage system files and to display software and boot information.

Commands by Usage

This chapter presents file management commands alphabetically. Use Table 102 to locate commands in this chapter based on their use.

Table 102 File Management Commands by Usage

Type	Command
Software Version	**reset system** on page 582
	display version on page 576
Boot Settings	**set boot partition** on page 587
	set boot configuration-file on page 586
	set boot backup-configuration on page 585
	display boot on page 573
	clear boot config on page 566
	clear boot backup-configuration on page 566
File Management	**dir** on page 570
	copy on page 567
	md5 on page 580
	delete on page 569
	mkdir on page 580
	rmdir on page 584
Configuration File	**save config** on page 584
	load config on page 578
	display config on page 574

Downloaded from www.Manualslib.com manuals search engine

Table 102 File Management Commands by Usage (continued)

Type	Command
System Backup and Restore	**backup** on page 564
	restore on page 583

backup

Creates an archive of WX system files and optionally, user file, in Unix *tape archive* (*tar*) format.

Syntax **`backup system [tftp:/ip-addr/]filename [all | critical]`**

Defaults — All.

Access — Enabled.

History —.

Usage — You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the **all** option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

Downloaded from www.Manualslib.com manuals search engine

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **display boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

Examples — The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
WX1200# backup system tftp:/10.10.20.9/sysa_bak critical

success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

Table 103 describes the fields.

Table 103 Output for backup

Field	Description
[**tftp:/***ip-addr***/**]*filename*	Name of the archive file to create. You can store the file locally in the switch's nonvolatile storage or on a TFTP server.
all	Backs up system files and all the files in the user files area. The user files area contains the set of files listed in the *file* section of **dir** command output.
critical	Backs up system files only, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less.

See Also

- **dir** on page 570
- **restore** on page 583

Downloaded from www.Manualslib.com manuals search engine

clear boot backup-configuration

Clears the filename specified as the backup configuration file. In the event that MSS cannot read the configuration file at boot time, a backup configuration file is not used.

Syntax — **`clear boot backup-configuration`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command clears the name specified as the backup configuration file from the configuration of the WX switch:

```
WX4400# clear boot backup-configuration
success: Backup boot config filename was cleared.
```

See Also

- **set boot backup-configuration** on page 585
- **display boot** on page 573

clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

Syntax — **`clear boot config`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following commands back up the configuration file on an WX switch, reset the switch to its factory default configuration, and reboot the switch:

```
WX4400# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# clear boot config
success: Reset boot config to factory defaults.
```

Downloaded from www.Manualslib.com manuals search engine

```
WX4400# reset system force
...... rebooting ......
```

See Also

- **display config** on page 574
- **reset system** on page 582

---

copy

Performs the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

Syntax — **copy** *source-url destination-url*

- *source-url* — Name and location of the file to copy. The uniform resource locator (URL) can be one of the following:
  - [*subdirname/*]*filename*
  - **file:**[*subdirname/*]*filename*
  - **tftp://ip-addr/**[*subdirname/*]*filename*
  - **tmp:***filename*

  For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation.

  The *subdirname/* option specifies a subdirectory.
- *destination-url* — Name of the copy and the location where to place the copy. The URL can be one of the following:
  - [*subdirname/*]*filename*
  - **file:**[*subdirname/*]*filename*
  - **tftp://***ip-addr/*[*subdirname/*]*filename*

  If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following:
  - **boot0:**/*filename*
  - **boot1:**/*filename*

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The *filename* and **file:***filename* URLs are equivalent. You can use either URL to refer to a file in an WX switch's nonvolatile memory. The **tftp://***ip-addr***/***filename* URL refers to a file on a TFTP server. If DNS is configured on the WX switch, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:***filename* URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:/***filename* or **boot1:/***filename*. You must specify the boot partition that *was not* used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples — The following command copies a file called *floorwx* from nonvolatile storage to a TFTP server:

```
WX4400# copy floorwx tftp://10.1.1.1/floorwx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called *closetwx* from a TFTP server to nonvolatile storage:

```
WX4400# copy tftp://10.1.1.1/closetwx closetwx
success: received 637 bytes in 0.253 seconds [ 2517
bytes/sec]
```

The following command copies system image *WXA03001.Rel* from a TFTP server to boot partition 1 in nonvolatile storage:

```
WX4400# copy tftp://10.1.1.107/WXA03001.Rel
boot1:WXA03001.Rel
.....................................................
.....................................success:
received 9163214 bytes in 105.939 seconds [ 86495 bytes/sec]
```

Downloaded from www.Manualslib.com manuals search engine

The following commands rename *test-config* to *new-config* by copying it from one name to the other in the same location, then deleting *test-config*:

```
WX4400# copy test-config new-config
WX4400# delete test-config
success: file deleted.
```

The following command copies file *corpa-login.html* from a TFTP server into subdirectory *corpa* in a WX switch's nonvolatile storage:

```
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

See Also

- **delete** on page 569
- **dir** on page 570

delete

Deletes a file.

CAUTION: *MSS does not prompt you to verify whether you want to delete a file. When you press Enter after typing a* ***delete*** *command, MSS immediately deletes the specified file.*

MSS does not allow you to delete the currently running software image file or the running configuration.

Syntax — **`delete`** *`url`*

- *`url`* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

  If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **subdir_a/file_a**.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You might want to copy the file to a TFTP server as a backup before deleting the file.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands copy file *testconfig* to a TFTP server and delete the file from nonvolatile storage:

```
WX4400# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# delete testconfig
success: file deleted.
```

The following commands delete file *dang_doc* from subdirectory *dang*:

```
WX4400# delete dang/dang_doc
success: file deleted.
```

See Also

- **copy** on page 567
- **dir** on page 570

dir

Displays a list of the files in nonvolatile storage and temporary files.

Syntax — **dir** [*subdirname*] **[file:] | [core:] | [boot0:] | [boot1:]**

- *subdirname* — Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories.
- **file** — Limits **dir** output to the contents of the user files area.
- **core:** — Limits **dir** output to the contents of the */tmp/core* subdirectory.
- **boot0:** — Limits **dir** output to the contents of the *boot0* partition.
- **boot1:** — Limits **dir** output to the contents of the *boot1* partition

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Core; file; boot0 and boot1 options added, to limit the output to the specified category, in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays the files in the root directory:

```
WX4400# dir
================================================================================
file:
Filename                                          Size          Created
file:configuration                                 48 KB      Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                              17 KB      Mar 14 2005, 22:20:04
corp_a/                                           512 bytes   May 21 2004, 19:15:48
file:dangcfg                                       14 KB      Mar 14 2005, 22:20:04
old/                                              512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005                        40 KB      May 09 2005, 21:08:30
file:sysa_bak                                      12 KB      Mar 15 2005, 19:18:44
file:testback                                      28 KB      Apr 19 2005, 16:37:18
Total:         159 Kbytes used, 207663 Kbytes free
================================================================================
Boot:
Filename                                          Size          Created
boot0:mx040100.020                               9780 KB      Aug 23 2005, 15:54:08
*boot1:mx040100.020                              9796 KB      Aug 28 2005, 21:09:56
Boot0: Total:        9780 Kbytes used, 2460 Kbytes free
Boot1: Total:        9796 Kbytes used, 2464 Kbytes free
================================================================================
temporary files:
Filename                                          Size          Created
core:command_audit.cur                             37 bytes   Aug 28 2005, 21:11:41
Total:          37 bytes used, 91707 Kbytes free
```

The following command displays the files in the *old* subdirectory:

```
WX4400# dir old
================================================================================
file:
Filename                                          Size          Created
file:configuration.txt                           3541 bytes   Sep 22 2003, 22:55:44
file:configuration.xml                             24 KB      Sep 22 2003, 22:55:44
Total:          27 Kbytes used, 207824 Kbytes free
```

Downloaded from www.Manualslib.com manuals search engine

The following command limits the output to the contents of the user files area:

```
WX4400# dir file:
================================================================================
file:
Filename                                          Size           Created
file:configuration                                 48 KB      Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                              17 KB      Mar 14 2005, 22:20:04
corp_a/                                           512 bytes   May 21 2004, 19:15:48
file:dangcfg                                       14 KB      Mar 14 2005, 22:20:04
dangdir/                                          512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005                        40 KB      May 09 2005, 21:08:30
file:sysa_bak                                      12 KB      Mar 15 2005, 19:18:44
file:testback                                      28 KB      Apr 19 2005, 16:37:18
Total:         159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the */tmp/core* subdirectory:

```
WX4400# dir core:
================================================================================
file:
Filename                                          Size           Created
core:command_audit.cur                             37 bytes   Aug 28 2005, 21:11:41
Total:          37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the *boot0* partition:

```
WX4400# dir boot0:
================================================================================
file:
Filename                                          Size           Created
boot0:mx040100.020                               9780 KB      Aug 23 2005, 15:54:08
Total:        9780 Kbytes used, 207663 Kbytes free
```

Table 104 describes the fields in the **dir** output.

Downloaded from www.Manualslib.com manuals search engine

Table 104 Output for dir

Field	Description
Filename	Filename or subdirectory name. For files, the directory name is shown in front of the filename (for example, file:configuration). The *file:* directory is the root directory. For subdirectories, a forward slash is shown at the end of the subdirectory name (for example, old/). In the boot partitions list (Boot:), an asterisk (*) indicates the boot partition from which the currently running image was loaded and the image filename.
Size	Size in Kbytes or bytes.
Created	System time and date when the file was created or copied onto the switch.
Total	Number of kilobytes in use to store files and the number that are still free.

See Also

- **copy** on page 567
- **delete** on page 569

display boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax — **`display boot`**

Defaults — None.

Access — Access.

History —Introduced in MSS Version 3.0. New fields, Configured boot version and Backup boot configuration added in MSS Version 4.0.

Examples — The following command shows the boot information for a WX switch:

```
WX1200# display boot
Configured boot version:         4.1.0.65
Configured boot image:           boot1:mx040100.020
Configured boot configuration:   file:configuration
Backup boot configuration:       file:backup.cfg
Booted version:                  4.1.0.65
Booted image:                    boot1:mx040100.020
```

Downloaded from www.Manualslib.com manuals search engine

```
Booted configuration:            file:configuration
Product model:                   WX
```

Table 105 describes the fields in the **display boot** output.

Table 105 Output for display boot

Field	Description
Configured boot version	Software version the switch will run next time the software is rebooted.
Configured boot image	Boot partition and image filename MSS will use to boot next time the software is rebooted.
Configured boot configuration	Configuration filename MSS will use to boot next time the software is rebooted.
Backup boot configuration	The name of the configuration file to be used in the event that MSS cannot read the configured boot configuration file next time the software is rebooted.
Booted version	Software version the switch is running.
Booted image	Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image.
Booted configuration	Configuration filename MSS used to load the configuration the last time the software was rebooted.

See Also

- **display version** on page 576
- **reset system** on page 582
- **set boot configuration-file** on page 586

display config

Displays the configuration running on the WX switch.

Syntax — **display config** [**area** *area*] [*all*]

- **area** *area* — Configuration area. You can specify one of the following:
  - **aaa**
  - **acls**
  - **ap**
  - **arp**
  - **eapol**

Downloaded from www.Manualslib.com manuals search engine

- **httpd**
- **ip**
- **ip-config**
- **log**
- **mobility-domain**
- **ntp**
- **portconfig**
- **portgroup**
- **radio-profile**
- **rfdetect**
- **service-profile**
- **sm**
- **snmp**
- **snoop**
- **spantree**
- **system**
- **trace**
- **vlan**
- **vlan-fdb**

  If you do not specify a configuration area, nondefault information for all areas is displayed.

- **all** — Includes configuration items that are set to their default values.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. New options added for remote traffic monitoring (snoop) and **rfdevice** changed to **rfdetect** in MSS Version 4.0.

Usage — If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows configuration information for VLANs:

```
WX4400# display config area vlan
# Configuration nvgen'd at 2004-5-21 19:36:48
# Image 3.0.0
# Model WX4400
# Last change occurred at 2004-5-21 18:20:50
set vlan 1 port 1
```

See Also

- **load config** on page 578
- **save config** on page 584

display version

Displays software and hardware version information for an WX switch and, optionally, for any attached MAP access points.

Syntax — **display version** [**details**]

- **details** — Includes additional software build information and information about the MAP access points configured on the WX switch.

Defaults — None

Access — All.

History —Introduced in MSS Version 3.0.

Examples — The following command displays version information for a WX switch:

```
WX1200# display version

        Mobility System Software, Version: 4.1.0 QA 67
        Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights
reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Model:             WX
Hardware
   Mainboard:      version 24 ; revision 3 ; FPGA version 24
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
```

Downloaded from www.Manualslib.com manuals search engine

```
Flash:              4.1.0.14  - md0a
Kernel:             3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:         4.10 / 4.1.0
```

The following command displays additional software build information and MAP access point information:

```
WX1200# display version details

        Mobility System Software, Version: 4.1.0 QA 67
        Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights
reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Label:              4.1.0.67_072105_MX20
Build Suffix:       -d-O1
Model:              WX
Hardware
   Mainboard:       version 24 ; revision 3 ; FPGA version 24
   CPU Model:       750 (Revision 3.1)
   PoE board:       version 1 ; FPGA version 6
Serial number       0321300013
Flash:              4.1.0.14  - md0a
Kernel:             3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:         4.10 / 4.1.0

Port/DAP AP Model   Serial #       Versions
-------- ---------- -------------- ------------------------
11  /-   MP-352     0424902948     H/W  : A
                            F/W1 : 5.6
                            F/W2 : 5.6
                            S/W  : 4.1.0.67_072105_0432__AP
                        BOOT S/W : 4.0.3.15_062705_0107__AP
```

Table 106 describes the fields in the **display version** output.

Table 106 Output for display version

Field	Description
Build Information	Factory timestamp of the image file.
Label	Software version and build date.
Build Suffix	Build suffix.
Model	Build model.

Downloaded from www.Manualslib.com manuals search engine

Table 106 Output for display version (continued)

Field	Description
Hardware	Version information for the WX switch's motherboard and Power over Ethernet (PoE) board.
Serial number	Serial number of the WX switch.
Flash	Flash memory version.
Kernel	Kernel version.
BootLoader	Boot code version.
Port/DAP	Port number connected to a MAP access point.
AP Model	MAP model number.
Serial #	MAP serial number.
Versions	MAP hardware, firmware, and software versions.

See Also

- **display boot** on page 573

load config

Loads configuration commands from a file and replaces the WX switch's running configuration with the commands in the loaded file.

CAUTION: *This command completely removes the running configuration and replaces it with the configuration contained in the file. 3Com recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.*

Syntax — **`load config`** [*`url`*]

- *`url`* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

  If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults — The default file location is nonvolatile storage.

The current version supports loading a configuration file only from the switch's nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

Downloaded from www.Manualslib.com manuals search engine

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the WX switch used *configuration* for the most recent configuration load, MSS uses *configuration* again unless you specify a different filename. To display the filename of the configuration file MSS loaded during the last reboot, use the **display boot** command.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command completely replaces the running configuration with the configuration in the file.

Examples — The following command reloads the configuration from the most recently loaded configuration file:

```
WX4400# load config
Reloading configuration may result in lost of connectivity,
do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

The following command loads configuration file *testconfig1*:

```
WX4400# load config testconfig1
Reloading configuration may result in lost of connectivity,
do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

See Also

- **display boot** on page 573
- **display config** on page 574
- **save config** on page 584

Downloaded from www.Manualslib.com manuals search engine

md5

Calculates the MD5 checksum for a file in the switch's nonvolatile storage.

Syntax — **md5 [boot0: | boot1:]***filename*

- **boot0: | boot1:** — Boot partition into which you copied the file.
- *filename* — Name of the file.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

Examples — The following command calculates the checksum for image file WX040003.020 in boot partition 0:

```
pubs# md5 boot0:MX040003.020
MD5 (boot0:MX040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

See Also

- **copy** on page 567
- **dir** on page 570

mkdir

Creates a new subdirectory in nonvolatile storage.

Syntax — **mkdir** [*subdirname*]

- *subdirname* — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following commands create a subdirectory called *corp2* and display the root directory to verify the result:

```
WX4400# mkdir corp2
success: change accepted.
WX4400# dir
================================================================================
file:
Filename                                        Size           Created
file:configuration                               17 KB      May 21 2004, 18:20:53
file:configuration.txt                          379 bytes   May 09 2004, 18:55:17
corp2/                                          512 bytes   May 21 2004, 19:22:09
corp_a/                                         512 bytes   May 21 2004, 19:15:48
file:dangcfg                                     13 KB      May 16 2004, 18:30:44
dangdir/                                        512 bytes   May 16 2004, 17:23:44
old/                                            512 bytes   Sep 23 2003, 21:58:48
Total:          33 Kbytes used, 207822 Kbytes free
================================================================================
Boot:
Filename                                        Size           Created
*boot0:bload                                    746 KB      May 09 2004, 19:02:16
*boot0:WXA03002.Rel                  8182 KB      May 09 2004, 18:58:16
boot1:WXA03001.Rel                   8197 KB      May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
Total:         0 bytes used, 93537 Kbytes free
```

See Also

- **dir** on page 570
- **rmdir** on page 584

Downloaded from www.Manualslib.com manuals search engine

reset system

Restarts an WX switch and reboots the software.

Syntax — **reset system** [**force**]

- **force** — Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the WX switch but instead displays a message advising you to either save the configuration changes or use the **force** option.

Examples — The following command restarts an WX switch that does not have any unsaved configuration changes:

```
WX4400# reset system
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart an WX switch with a running configuration that has unsaved changes, and then force the switch to restart:

```
WX4400# reset system
error: Cannot reset, due to unsaved configuration changes.
Use "reset system force" to override.
WX4400# reset system force
...... rebooting ......
```

See Also

- **display boot** on page 573
- **display version** on page 576
- **save config** on page 584

Downloaded from www.Manualslib.com manuals search engine

restore

Unzips a system archive created by the backup command and copies the files from the archive onto the switch.

Syntax **`restore system [tftp:/ip-addr/]filename [all | critical]`**

Defaults — Critical.

Access — Enabled.

History —Introduced in MSS Version 3.2.

Usage — If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The restore command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

Note: *If the archive's files cannot fit on the switch, the restore operation fails. 3Com recommends deleting unneeded image files before creating or restoring an archive.*

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch's archive onto another switch.

CAUTION: *Do not use the force option unless you are certain you want to replace the switch's files with files from another switch. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.*

Examples — The following command restores system-critical files on a switch, from archive sysa_bak.

```
WX1200# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386
bytes/sec]
success: restore complete.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **backup** on page 564

rmdir

Removes a subdirectory from nonvolatile storage.

Syntax — **rmdir** [*subdirname*]

- *subdirname* — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

Examples — The following example removes subdirectory *corp2*:

```
WX4400# rmdir corp2
success: change accepted.
```

See Also

- **dir** on page 570
- **mkdir** on page 580

save config

Saves the running configuration to a configuration file.

Syntax — **save config** [*filename*]

- *filename* — Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces.

  To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults — By default, MSS saves the running configuration as the configuration filename used during the last reboot.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the **display boot** command.

The command completely replaces the specified configuration file with the running configuration.

Examples — The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is *configuration*.

```
WX4400# save config
Configuration saved to configuration.
```

The following command saves the running configuration to a file named *testconfig1*:

```
WX4400# save config testconfig1
Configuration saved to testconfig1.
```

See Also

- **display boot** on page 573
- **display config** on page 574
- **load config** on page 578

set boot backup-configuration

Specifies the name of a backup configuration file to be used in the event that MSS cannot read the WX switch's configuration file at boot time.

Syntax — **set boot backup-configuration** *filename*

- *filename* —Name of the file to use as a backup configuration file if MSS cannot read the WX switch's configuration file.

Defaults — By default, there is no backup configuration file.

Access — Enabled.

Downloaded from www.Manualslib.com manuals search engine

History —Introduced in MSS Version 4.1.

Examples — The following command specifies a file called backup.cfg as the backup configuration file on the WX switch:

```
WX1200# set boot backup-configuration backup.cfg
success: backup boot config filename set.
```

See Also

- **clear boot backup-configuration** on page 566
- **display boot** on page 573

set boot configuration-file

Changes the configuration file to load after rebooting.

Syntax — **set boot configuration-file** *filename*

- *filename* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

  To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults — The default configuration filename is *configuration*.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The file must be located in the switch's nonvolatile storage.

Examples — The following command sets the boot configuration file to *testconfig1*:

```
WX4400# set boot configuration-file testconfig1
success: boot config set.
```

Downloaded from www.Manualslib.com manuals search engine

set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

Syntax — **`set boot partition`** {**`boot0`** | **`boot1`**}

- **`boot0`** — Boot partition 0.
- **`boot1`** — Boot partition 1.

Defaults — By default, an WX switch uses the same boot partition for the next software reload that was used to boot the currently running image.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To determine the boot partition that was used to load the currently running software image, use the **dir** command.

Examples — The following command sets the boot partition for the next software reload to partition 1:

```
WX4400# set boot partition boot1
success: Boot partition set to boot1.
```

See Also

- **copy** on page 567
- **dir** on page 570
- **reset system** on page 582

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

21 TRACE COMMANDS

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the **set trace ?** command.

CAUTION: *Using the* ***set trace*** *command can have adverse effects on system performance. 3Com recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.*

Commands by Usage

This chapter presents trace commands alphabetically. Use Table 107 to locate commands in this chapter based on their use.

Table 107 Trace Commands by Usage

Type	Command
Trace	**set trace sm** on page 595
	set trace dot1x on page 594
	set trace authentication on page 592
	set trace authorization on page 593
	display trace on page 591
	save trace on page 592
	clear trace on page 590
	clear log trace on page 590

Downloaded from www.Manualslib.com manuals search engine

clear log trace

Deletes the log messages stored in the trace buffer.

Syntax — **`clear log trace`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To delete the trace log, type the following command:

```
WX4400# clear log trace
```

See Also

- **display log buffer** on page 610
- **set log** on page 614

clear trace

Deletes running trace commands and ends trace processes.

Syntax — **`clear trace`** {*`trace-area`* | **`all`**}

- *`trace-area`* — Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter:
  - **`authorization`** — Ends an authorization trace
  - **`dot1x`** — Ends an 802.1X trace
  - **`authentication`** — Ends an authentication trace
  - **`sm`** — Ends a session manager trace
- **`all`** — Ends all trace processes.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To clear all trace processes, type the following command:

```
WX4400# clear trace all
success: clear trace all
```

Downloaded from www.Manualslib.com manuals search engine

To clear the session manager trace, type the following command:

```
WX4400# clear trace sm
success: clear trace sm
```

See Also

- **display trace** on page 591
- **set trace authentication** on page 592
- **set trace authorization** on page 593
- **set trace dot1x** on page 594
- **set trace sm** on page 595

display trace

Displays information about traces that are currently configured on the WX switch, or all possible trace options.

Syntax — **display trace** [**all**]

- **all** — Displays all possible trace options and their configuration.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To view the traces currently running, type the following command:

```
WX4400# display trace
milliseconds spent printing traces: 1885.614
Trace Area           Level Mac               User              Port Filter
-------------------- ----- ----------------- ----------------- ---- --------
dot1x                    5                                            0
sm                       5                                            0
```

See Also

- **clear trace** on page 590
- **set trace authentication** on page 592
- **set trace authorization** on page 593
- **set trace dot1x** on page 594
- **set trace sm** on page 595

Downloaded from www.Manualslib.com manuals search engine

save trace

Saves the accumulated trace data for enabled traces to a file in the WX switch's nonvolatile storage.

Syntax — **save trace filename**

- *filename* — Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: *traces/trace1*

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — To save trace data into the file *trace1* in the subdirectory *traces*, type the following command:

```
WX4400# save trace traces/trace1
```

set trace authentication

Traces authentication information.

Syntax — **set trace authentication** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command starts a trace for information about user *jose's* authentication:

```
WX4400# set trace authentication user jose
success: change accepted.
```

See Also

- **clear trace** on page 590
- **display trace** on page 591

set trace authorization

Traces authorization information.

Syntax — **set trace authorization** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX a port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05:

```
WX4400# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear trace** on page 590
- **display trace** on page 591

---

set trace dot1x

Traces 802.1X sessions.

Syntax — **set trace dot1x** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
WX4400# set trace dot1x mac-addr 00:01:02:03:04:05:
success: change accepted.
```

See Also

- **clear trace** on page 590
- **display trace** on page 591

Downloaded from www.Manualslib.com manuals search engine

set trace sm

Traces session manager activity.

Syntax — **set trace sm** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.a

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05:

```
WX4400# set trace sm mac-addr 00:01:02:03:04:05:
success: change accepted.
```

See Also

- **clear trace** on page 590
- **display trace** on page 591

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

22 SNOOP COMMANDS

Use snoop commands to monitor wireless traffic, by using a Distributed MAP as a sniffing device. The MAP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

(For more information, including setup instructions for the monitoring station, see the "Remotely Monitoring Traffic" section in the "Troubleshooting a WX Switch" chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

Commands by Usage

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 108 Remote Monitoring (Snooping) Commands By Usage

Remote monitoring (snooping)	**set snoop** on page 599
	display snoop info on page 604
	clear snoop on page 598
	set snoop map on page 602
	display snoop map on page 605
	display snoop on page 604
	clear snoop map on page 598
	set snoop mode on page 603
	display snoop stats on page 606

Downloaded from www.Manualslib.com manuals search engine

clear snoop

Deletes a snoop filter.

Syntax — `clear snoop` *`filter-name`*

- *`filter-name`* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command deletes snoop filter *snoop1*:

```
WX1200# clear snoop snoop1
```

See Also

- **set snoop** on page 599
- **display snoop info** on page 604

clear snoop map

Removes a snoop filter from a MAP radio.

Syntax — `clear snoop map` *`filter-name`* `dap` *`dap-num`* `radio {1 | 2}`

- *`filter-name`* — Name of the snoop filter.
- **`dap`** *`dap-num`* — Number of a Distributed MAP to which to snoop filter is mapped
- **`radio 1`** — Radio 1 of the MAP.
- **`radio 2`** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Examples — The following command removes snoop filter *snoop2* from radio 2 on Distributed MAP 3:

Downloaded from www.Manualslib.com manuals search engine

```
WX1200# clear snoop map snoop2 dap 3 radio 2
success: change accepted.
```

The following command removes all snoop filter mappings from all radios:

```
WX1200# clear snoop map all
success: change accepted.
```

See Also

- **set snoop map** on page 602
- **display snoop** on page 604
- **display snoop map** on page 605

---

set snoop

Configures a snoop filter.

Syntax — **set snoop** *filter-name* **[***condition-list***] [observer** *ip-addr***] [snap-length** *num***]**

- *filter-name* — Name for the filter. The name can be up to 32 alphanumeric characters, with no spaces.
- *condition-list* — Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination:
  - **frame-type {eq | neq} {beacon | control | data | management | probe}**
  - **channel {eq | neq} channel**
  - **bssid {eq | neq} bssid**
  - **src-mac {eq | neq} mac-addr**
  - **dest-mac {eq | neq} mac-addr**
  - **host-mac {eq | neq} mac-addr**
  - **mac-pair mac-addr1 mac-addr2**

Downloaded from www.Manualslib.com manuals search engine

To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option. To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit **frame-type**, all frame types match the filter.

For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value.

- **observer** *ip-addr* — Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the MAP radio still counts the packets that match the filter.
- **snap-length** *num* — Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. 3Com recommends specifying a snap length of 100 bytes or less.

Defaults — No snoop filters are configured by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the MAP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.
- If the snoop filter is running on a Distributed MAP, and the MAP used a DHCP server in its local subnet to configure its IP information, and the MAP did not receive a default gateway address as a result, the observer must also be in the same subnet. Without a default gateway, the MAP cannot find the observer.

Downloaded from www.Manualslib.com manuals search engine

- The MAP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the MAP to the observer. If the observer is not present, the MAP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the MAP. These ICMP messages can affect network and MAP performance.

Examples — The following command configures a snoop filter named *snoop1* that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
WX1200# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named *snoop2* that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
WX1200# set snoop snoop2 frame-type eq data mac-pair
aa:bb:cc:dd:ee:ff 11:22:33:44:55:66 observer 10.10.30.3
snap-length 100
```

See Also

- **clear snoop** on page 598
- **set snoop map** on page 602
- **set snoop mode** on page 603
- **display snoop info** on page 604
- **display snoop stats** on page 606

Downloaded from www.Manualslib.com manuals search engine

set snoop map

Maps a snoop filter to a radio on a Distributed MAP. A snoop filter does take effect until you map it to a radio and enable the filter.

Syntax — **`set snoop map`** *`filter-name`* **`dap`** *`dap-num`* **`radio {1 | 2}`**

- *`filter-name`* — Name of the snoop filter.
- **`dap`** *`dap-num`* — Number of a Distributed MAP to which to map the snoop filter.
- **`radio 1`** — Radio 1 of the MAP.
- **`radio 2`**— Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — Snoop filters are unmapped by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the MAP sends only one copy of a packet that matches a filter to the observer. After the first match, the MAP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the MAP still maintains a counter of the number of packets that match the filter. (See **display snoop stats** on page 606.)

Examples — The following command maps snoop filter *snoop1* to radio 2 on Distributed MAP 3:

```
WX1200# set snoop map snoop1 dap 3 radio 2
success: change accepted.
```

See Also

- **clear snoop map** on page 598
- **set snoop** on page 599
- **set snoop mode** on page 603
- **display snoop map** on page 605
- **display snoop stats** on page 606

Downloaded from www.Manualslib.com manuals search engine

set snoop mode

Enables a snoop filter. A snoop filter does not take effect until you map it to a MAP radio and enable the filter.

Syntax — **`set snoop {`***`filter-name`* **`| all}`**
`mode {enable [stop-after` *`num-pkts`***`] | disable}`**

- *`filter-name`* **`| all`** — Name of the snoop filter. Specify **all** to enable all snoop filters.
- **`enable [stop-after`** *`num-pkts`***`]`** — Enables the snoop filter.

  The **stop-after** option disables the filter after the specified number of packets match the filter. Without the stop-after option, the filter operates until you disable it or until the MAP is restarted.
- **`disable`** — Disables the snoop filter.

Defaults — Snoop filters are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The filter mode is not retained if you change the filter configuration or disable and reenable the radio, or when the MAP or the WX switch is restarted. You must reenable the filter to place it back into effect.

Examples — The following command enables snoop filter *snoop1*, and configures the filter to stop after 5000 packets match the filter:

```
WX1200# set snoop snoop1 mode enable stop-after 5000
success: filter 'snoop1' enabled
```

See Also

- **display snoop** on page 604
- **display snoop info** on page 604
- **display snoop map** on page 605
- **display snoop stats** on page 606

Downloaded from www.Manualslib.com manuals search engine

display snoop

Displays the MAP radio mapping for all snoop filters.

Syntax — **`display snoop`**

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — To display the mappings for a specific MAP radio, use the **display snoop map** command.

Examples — The following command shows the MAP radio mappings for all snoop filters configured on a WX switch:

```
WX1200# display snoop
Dap: 3          Radio: 2
        snoop1
        snoop2
Dap: 2          Radio: 2
        snoop2
```

See Also

- **clear snoop map** on page 598
- **set snoop map** on page 602
- **display snoop map** on page 605

display snoop info

Shows the configured snoop filters.

Syntax — **`display snoop`** *`filter-name`*

- *`filter-name`* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command shows the snoop filters configured in the examples above:

```
WX1200# display snoop info
snoop1:
        observer 10.10.30.2 snap-length 100
        all packets
snoop2:
        observer 10.10.30.3 snap-length 100
        frame-type eq data
        mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

See Also

- **clear snoop** on page 598
- **set snoop** on page 599

display snoop map

Shows the MAP radios that are mapped to a specific snoop filter.

Syntax — **display snoop map** *filter-name*

- *filter-name* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — To display the mappings for all snoop filters, use the **display snoop** command.

Examples — The following command shows the mapping for snoop filter *snoop1*:

```
WX1200# display snoop map snoop1
filter 'snoop1' mapping
        Dap: 3          Radio: 2
```

See Also

- **clear snoop map** on page 598
- **set snoop map** on page 602
- **display snoop** on page 604

Downloaded from www.Manualslib.com manuals search engine

display snoop stats

Displays statistics for enabled snoop filters.

Syntax — **display snoop stats [***filter-name* **[***dap-num* **[radio {1 | 2}]]]**

- *filter-name* — Name of the snoop filter.
- *dap-num* — Number of a Distributed MAP to which the snoop filter is mapped
- **radio 1** — Radio 1 of the MAP
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The MAP retains statistics for a snoop filter until the filter is changed or disabled. The MAP then clears the statistics.

Examples — The following command shows statistics for snoop filter *snoop1*:

```
WX1200# display snoop stats snoop1
Filter          Dap Radio   Rx Match     Tx Match     Dropped        Stop-After
================================================================================
snoop1            3     1            96           4            0      stopped
```

Downloaded from www.Manualslib.com manuals search engine

Table 109 describes the fields in this display.

Table 109 display snoop stats Output

Field	Description
Filter	Name of the snoop filter.
Dap	Distributed MAP containing the radio to which the filter is mapped.
Radio	Radio to which the filter is mapped.
Rx Match	Number of packets received by the radio that match the filter.
Tx Match	Number of packets sent by the radio that match the filter.
Dropped	Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.
Stop-After	Filter state: ▪ running—enabled ▪ stopped—disabled ▪ *number-of-packets*—If the filter is running and the stop-after option was used to stop the filter, this field displays the number of packets that still need to match before the filter is stopped.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

23 SYSTEM LOG COMMANDS

Use the system log commands to record information for monitoring and troubleshooting. MSS system logs are based on RFC 3164, which defines the log protocol.

Commands by Usage

This chapter present system log commands alphabetically. Use Table 110 to locate commands in this chapter based on their use.

Table 110 System Log Commands by Usage

Type	Command
System Logs	**set log** on page 614
	set log mark on page 616
	display log config on page 612
	display log buffer on page 610
	display log trace on page 613
	clear log on page 609

clear log

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

Syntax — **`clear log`** [**`buffer`** | **`server`** *`ip-addr`*]

- **`buffer`** — Deletes the log messages stored in nonvolatile storage.
- **`server`** *`ip-addr`* — Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

Defaults — None.

Downloaded from www.Manualslib.com manuals search engine

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
WX4400# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
WX4400# clear log buffer
success: change accepted.
```

See Also

- **clear log trace** on page 590
- **set log** on page 614

display log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax — **display log buffer** [{**+**|**-**}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

- **buffer** — Displays the log messages in nonvolatile storage.
- **+**|**-** *number-of-messages* — Displays the number of messages specified as follows:
  - A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log.
  - A negative number (for example, **-100**) displays that number of log entries starting from newest in the log.
- **facility** *facility-name* — Area of MSS that is sending the log message. Type a space and a question mark (**?**) after display **log buffer facility** for a list of valid facilities.
- **matching** *string* — Displays messages that match a string—for example, a username or IP address.

Downloaded from www.Manualslib.com manuals search engine

- **severity** *severity-level* — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
  - **emergency** — The WX switch is unusable.
  - **alert** — Action must be taken immediately.
  - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  - **error** — The WX is missing data or is unable to form a connection.
  - **warning —** A possible problem exists.
  - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  - **info** — Informational messages only. No problem exists.
  - **debug** — Output from debugging.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by 3Com for troubleshooting and are not intended for administrator use.

Examples — Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
WX4400# display log buffer facility ?
<facility name>             Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,
ASO, BOOT, CLI, CLUSTER, COPP, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY, HTTPD,
IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE,
SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MAP,
RAPDA, WEBVIEW, EAP, FP, STAT, SSHD, SUP, DNSD, CONFIG, BACKUP.
```

The following command displays logged messages for the AAA facility:

```
WX4400# display log buffer facility AAA
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM
special event (98) on locality 3950 which is gone
```

Downloaded from www.Manualslib.com manuals search engine

See Also

- **clear log** on page 609
- **display log config** on page 612

display log config

Displays log configuration information.

Syntax — **`display log config`**

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display how logging is configured, type the following command:

```
WX4400# display log config
Logging console:               disabled
Logging console severity:      DEBUG
Logging sessions:              disabled
Logging sessions severity:     INFO
Logging buffer:                enabled
Logging buffer severity:       DEBUG
Logging trace:                 enabled
Logging trace severity:        DEBUG
Logging buffer size:           10485760 bytes
Log marking:                    disabled
Log marking severity:           NOTICE
Log marking interval            300 seconds
Logging server:                10.1.1.10       severity DEBUG
Current session:                 disabled
Current session severity:        INFO
```

See Also

- **set log** on page 614
- **clear log** on page 609

Downloaded from www.Manualslib.com manuals search engine

display log trace

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax — **`display log trace`** [{**`+`**|**`-`**|**`/`**}*`number-of-messages`*] [**`facility`** *`facility-name`*] [**`matching`** *`string`*] [**`severity`** *`severity-level`*]

- **`trace`** — Displays the log messages in the trace buffer.
- **`+`**|**`-`**|**`/`***`number-of-messages`* — Displays the number of messages specified as follows:
  - A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log.
  - A negative number (for example, **-100**) displays that number of log entries starting from newest in the log.
  - A number preceded by a slash (for example, **/100**) displays that number of the most recent log entries in the log, starting with the least recent.
- **`facility`** *`facility-name`* — Area of MSS that is sending the log message. Type a space and a question mark **(?)** after **display log trace facility** for a list of valid facilities.
- **`matching`** *`string`* — Displays messages that match a string—for example, a username or IP address.
- **`severity`** *`severity-level`* — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
  - **`emergency`** — The WX switch is unusable.
  - **`alert`** — Action must be taken immediately.
  - **`critical`** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  - **`error`** — The WX is missing data or is unable to form a connection.
  - **`warning`** — A possible problem exists.
  - **`notice`** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  - **`info`** — Informational messages only. No problem exists.
  - **`debug`** — Output from debugging.

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
WX4400# display log trace facility ?
<facility name>             Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,
ASO, BOOT, CLI, CLUSTER, COPP, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY, HTTPD,
IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE,
SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MAP,
RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

See Also

- **clear log** on page 609
- **display log config** on page 612

set log

Enables or disables logging of WX and MAP events to the WX log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax — **set log** {**buffer** | **console** | **current** | **server** *ip-addr* | **sessions** | **trace**} [**severity** *severity-level*] **enable** | **disable**]

Syntax — **set log server** *ip-addr* [**severity** *severity-level* [**local-facility** *facility-level*]] [**enable** | **disable**]

- **buffer** — Sets log parameters for the log buffer in nonvolatile storage.
- **console** — Sets log parameters for console sessions.
- **current** — Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
- **server** *ip-addr* — Sets log parameters for a syslog server. Specify an address in dotted decimal notation.
- **sessions** — Sets the default log values for Telnet sessions. You can set defaults for the following log parameters:
  - Severity

Downloaded from www.Manualslib.com manuals search engine

- Logging state (enabled or disabled)

To override the session defaults for an individual session, type the **set log** command from within the session and use the **current** option.

- **trace** — Sets log parameters for trace files.
- **severity** *severity-level* — Logs events at a severity level greater than or equal to the level specified. Specify one of the following:
  - **emergency** — The WX switch is unusable.
  - **alert** — Action must be taken immediately.
  - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  - **error** — The WX is missing data or is unable to form a connection.
  - **warning** — A possible problem exists.
  - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  - **info** — Informational messages only. No problem exists.
  - **debug** — Output from debugging.
- **local-facility** *facility-level* — For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values:
  - **0** — maps all messages to *local0*.
  - **1** — maps all messages to *local1*.
  - **2** — maps all messages to *local2*.
  - **3** — maps all messages to *local3*.
  - **4** — maps all messages to *local4*.
  - **5** — maps all messages to *local5*.
  - **6** — maps all messages to *local6*.
  - **7** — maps all messages to *local7*.

  If you do not specify a local facility, MSS sends the messages with their default MSS facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.
- **enable** — Enables messages to the specified target.
- **disable** — Disables messages to the specified target.

Downloaded from www.Manualslib.com manuals search engine

Defaults — The following are defaults for the **set log** commands.

- Events at the error level and higher are logged to the WX console.
- Events at the error level and higher are logged to the WX system buffer.
- Trace logging is enabled, and debug-level output is stored in the WX trace buffer.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Using the command with only **enable** or **disable** turns logging on or off for the target at all levels. For example, entering **set log buffer enable** with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering **set log buffer disable** with no other keywords turns off all logging to the buffer.

Examples — To log only emergency, alert, and critical system events to the console, type the following command:

```
WX4400# set log console severity critical enable
success: change accepted.
```

See Also

- **clear log** on page 609
- **display log config** on page 612

set log mark

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. 3Com can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

Syntax — **set log mark [enable | disable] [severity** *level*] **[interval** *interval*]

- **enable** — Enables the mark messages.
- **disable** — Disables the mark messages.
- **severity** *level* — Log severity at which the messages are logged:
  - **emergency**

Downloaded from www.Manualslib.com manuals search engine

  - **alert**
  - **critical**
  - **error**
  - **warning**
  - **notice**
  - **info**
  - **debug**
- **interval** *interval* — Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

Defaults — Mark messages are disabled by default. When they are enabled, MSS generates a message at the notice level once every 300 seconds by default.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command enables mark messages:

```
WX1200# set log mark enable
success: change accepted.
```

See Also

- **display log config** on page 612

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

24 BOOT PROMPT COMMANDS

Boot prompt commands enable you to perform basic tasks, including booting a system image file, from the boot prompt (boot>). A CLI session enters the boot prompt if MSS does not boot successfully or you intentionally interrupt the boot process. To interrupt the boot process, press **q** followed by **Enter** (return).

CAUTION: *Generally, boot prompt commands are used only for troubleshooting. 3Com recommends that you use these commands only when working with 3Com Technical Support to diagnose a system issue. In particular, commands that change boot parameters can interfere with a WX switch's ability to boot successfully.*

Boot Prompt Commands by Usage

This chapter presents boot prompt commands alphabetically. Use Table 111 to locate commands in this chapter based on their use.

Table 111 Boot Prompt Commands by Usage

Type	Command
Command Information	**ls** on page 632
	help on page 631
Booting	**boot** on page 621
	reset on page 634
	autoboot on page 620
	dhcp on page 626
File Management	**dir** on page 627
	fver on page 630
	version on page 636

Downloaded from www.Manualslib.com manuals search engine

Table 111 Boot Prompt Commands by Usage (continued)

Type	Command
Boot Profile Management	**display** on page 628
	create on page 624
Boot Profile Management, cont.	**next** on page 633
	change on page 623
	delete on page 625
Diagnostics	**diag** on page 627
	test on page 635

autoboot

Displays or changes the state of the autoboot option. The autoboot option controls whether a WX switch automatically boots a system image after initializing the hardware, following a system reset or power cycle.

Syntax — **`autoboot [ON | on | OFF | off]`**

- **`ON`** — Enables the autoboot option.
- **`on`** — Same effect as **`ON`**.
- **`OFF`** — Disables the autoboot option.
- **`off`** — Same effect as **`OFF`**.

Defaults — The autoboot option is enabled by default.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Examples — The following command displays the current setting of the autoboot option:

```
boot> autoboot
The autoboot flag is on.
```

See Also

- **boot** on page 621

Downloaded from www.Manualslib.com manuals search engine

boot

Loads and executes a system image file.

Syntax — **boot** [**BT=***type*] [**DEV=***device*] [**FN=***filename*] [**HA=***ip-addr*] [**FL=***num*] [**OPT=***option*] [**OPT+=***option*]

- **BT=***type* — Boot type:
  - **c** — Compact flash. Boots using nonvolatile storage or a flash card.
  - **n** — Network. Boots using a TFTP server.
- **DEV=***device* — Location of the system image file:
  - **c:** — Nonvolatile storage area containing boot partition 0
  - **d:** — Nonvolatile storage area containing boot partition 1
  - **e:** — Primary partition of the flash card in the flash card slot
  - **f:** — Secondary partition of the flash card in the flash card slot
  - **boot0** — boot partition 0
  - **boot1** — boot partition 1
- **FN=***filename* — System image filename.
- **HA=***ip-addr* — Host address (IP address) of a TFTP server. This parameter applies only when the boot type is **n** (network).
- **FL=***num* — Number representing the bit settings of boot flags to pass to the booted system image. Use this parameter only if advised to do so by 3Com.
- **OPT=***option* — String up to 128 bytes of boot options to pass to the booted system image *instead of* the boot option(s) in the currently active boot profile. The options temporarily replace the options in the boot profile. Use this parameter only if advised to do so by 3Com.
- **OPT+=***option* — String up to 128 bytes of boot options to pass to the booted system image *in addition to* the boot option(s) in the currently active boot profile. The options are appended to the options already in the boot profile. Use this parameter only if advised to do so by 3Com.

Defaults — The boot settings in the currently active boot profile are used by default.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **display** command. To change the currently active boot profile, use the **change** command.

Examples — The following command loads system image file WXA30001.Rel from boot partition 1:

```
boot> boot FN=WXA03001.Rel DEV=boot1
Compact Flash load from boot0:WXA03001.Rel.
unzip: Inflating ramdisk_3.0.1_092304_WX4400 OK
unzip file len 36196930 OK


Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
    The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California.  All rights reserved.

Detecting hardware...done.
readclock: 2004-9-29 21:45:7.31 UTC
system initialized (3.0.1), starting MSS
Executing update_3
Starting supervisor 3.0.1_092304_WX4400 ...

SNMPD Sep 29 21:45:34.262293 NOTICE  SNMPD: SNMP Agent Resident Module Version
16.1.0.0
SNMPD Sep 29 21:45:34.263146 NOTICE  SNMPD: Copyright (c) 2004 3Com Corporation.
 All rights reserved.
SYS Sep 29 21:45:36.849457 NOTICE Port 1 up 1000 Full Duplex
SYSLOGD Sep 29 21:45:38.857125 ALERT SYSTEM_READY: The system has finished
booting. (cause was "Warm Reboot")


Copyright (c) 2004 3Com Corporation. All rights reserved.


Username:
```

See Also

- **change** on page 623
- **display** on page 628

Downloaded from www.Manualslib.com manuals search engine

change

Changes parameters in the currently active boot profile. (For information about boot profiles, see **display** on page 628.)

Syntax — **`change`**

Defaults — The default boot type is **c** (compact flash). The default filename is *default*. The default flags setting is 0x00000000 (all flags disabled) and the default options list is run=nos;boot=0. The default device setting is the boot partition specified by the most recent **set boot partition** command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — After you type the **change** command, the system interactively displays the current setting of each parameter and prompts you for the new setting. When prompted, type the new setting, press Enter to accept the current setting, or type **.** (period) to change the setting to its default value. To back up to the previous parameter, type **-** (hyphen).

For information about each of the boot parameters you can set, see **display** on page 628.

Examples — The following command enters the configuration mode for the currently active boot profile, changes the device to **boot1**, and leaves the other parameters with their current settings:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)

BOOT TYPE:     [c]
DEVICE:        [boot0:]boot1
FILENAME:      [default]
FLAGS:         [0x00000000]
OPTIONS:       [run=nos;boot=0]
```

Downloaded from www.Manualslib.com manuals search engine

The following command enters the configuration mode for the currently active boot profile and configures the WX switch (in this example, an WXR100) to boot using a TFTP server:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)y

BOOT TYPE:     [c]> n
DEVICE:        [boot0:]> emac1
FILENAME:      [default]> bootfile
HOST IP:       [0.0.0.0]> 172.16.0.1
LOCAL IP:      [0.0.0.0]> 172.16.0.21
GATEWAY IP:    [0.0.0.0]> 172.16.0.20
IP MASK:       [0.0.0.0]> 255.255.255.0
FLAGS:         [0x00000000]>
OPTIONS:       [run=nos;boot=0]>
```

See Also

- **boot** on page 621
- **create** on page 624
- **delete** on page 625
- **dhcp** on page 626
- **display** on page 628
- **next** on page 633

create

Creates a new boot profile. (For information about boot profiles, see **display** on page 628.)

Syntax — **`create`**

Defaults — The new boot profile has the same settings as the currently active boot profile by default.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — A WX switch can have up to four boot profiles. The boot profiles are stored in slots, numbered 0 through 3. When you create a new profile, the system uses the next available slot for the profile. If all four slots already contain profiles and you try to create a fifth profile, the switch displays a message advising you to change one of the existing profiles instead.

To make a new boot profile the currently active boot profile, use the **next** command. To change boot parameter settings, use the **change** command.

Examples — The following command creates a new boot profile in slot 1 on a WX switch that currently has only one boot profile, in slot 0:

```
boot> create

    BOOT Index:   1
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

See Also

- **change** on page 623
- **delete** on page 625
- **display** on page 628
- **next** on page 633

delete

Removes the currently active boot profile. (For information about boot profiles, see **display** on page 628.)

Syntax — **`delete`**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Usage — When you type the **delete** command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type **delete** to delete profile 3. You cannot delete boot profile 0.

Examples — To remove the currently active boot profile, type the following command:

```
boot> delete

    BOOT Index:    1
    BOOT TYPE:     c
    DEVICE:        boot1:
    FILENAME:      default
    FLAGS:         00000000
    OPTIONS:       run=nos;boot=0
```

See Also

- **change** on page 623
- **create** on page 624
- **display** on page 628
- **next** on page 633

dhcp

Displays or changes the state of the DHCP option. The DHCP option controls whether a WX switch uses DCHP to obtain its IP address when it is booted using a TFTP server.

Syntax — **dhcp [ON | on | OFF | off]**

- **ON** — Enables the DHCP option.
- **on** — Same effect as **ON**.
- **OFF** — Disables the DHCP option.
- **off** — Same effect as **OFF**.

Defaults — The DHCP option is disabled by default.

Access — Boot prompt.

History —Introduced in MSS Version 1.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

See Also

- **boot** on page 621

diag

Accesses the diagnostic mode.

Syntax — **`diag`**

Defaults — The diagnostic mode is disabled by default.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by 3Com.

dir

Displays the boot code and system image files on a WX switch.

Syntax — **`dir`** [**`c:`** | **`d:`** | **`e:`** | **`f:`** | **`boot0`** | **`boot1`**]

- **`c:`** — Nonvolatile storage area containing boot partition 0 (primary).
- **`d:`** — Nonvolatile storage area containing boot partition 1 (secondary).
- **`e:`** — Primary partition of the flash card in the flash card slot.
- **`f:`** — Secondary partition of the flash card in the flash card slot.
- **`boot0`** — Boot partition 0.
- **`boot1`** — Boot partition 1.

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — To display the system image software versions, use the **fver** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Examples — The following command displays all the boot code and system image files on a WX switch:

```
boot> dir

Internal Compact Flash Directory (Primary):
        WXA30001.Rel                8863722 bytes

  Internal Compact Flash Directory (Secondary):
        WXA30001.Rel                8862885 bytes
```

See Also

- **fver** on page 630
- **version** on page 636

display

Displays the currently active boot profile. A boot profile is a set of parameters that a WX switch uses to control the boot process. Each boot profile contains the following parameters:

- **Boot type** — Either compact flash (local device on the WX switch) or network (TFTP)
- **Boot device** — Location of the system image file
- **Filename** — System image file
- **Flags** — Number representing the bit settings of boot flags to pass to the booted system image.
- **Options** — String up to 128 bytes of boot options to pass to the booted system image

Downloaded from www.Manualslib.com manuals search engine

A WX switch can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

Syntax — **`display`**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Examples — To display the currently active boot profile, type the following command at the boot prompt:

```
boot> display

    BOOT Index:    0
    BOOT TYPE:     c
    DEVICE:        boot1:
    FILENAME:      default
    FLAGS:         00000000
    OPTIONS:       run=nos;boot=0
```

Table 112 describes the fields in the display.

Table 112 Output of display command

Field	Description
BOOT Index	Boot profile slot, which can be a number from 0 to 3.
BOOT TYPE	Boot type: ▪ **c** — Compact flash. Boots using nonvolatile storage or a flash card. ▪ **n** — Network. Boots using a TFTP server.

Downloaded from www.Manualslib.com manuals search engine

Table 112 Output of display command (continued)

Field	Description
DEVICE	Location of the system image file: ■ **c:** — Nonvolatile storage area containing boot partition 0 ■ **d:** — Nonvolatile storage area containing boot partition 1 ■ **e:** — Primary partition of the flash card in the flash card slot ■ **f:** — Secondary partition of the flash card in the flash card slot ■ **boot0** — boot partition 0 ■ **boot1** — boot partition 1
FILENAME	System image file name.
FLAGS	Number representing the bit settings of boot flags to pass to the booted system image.
OPTIONS	String up to 128 bytes of boot options to pass to the booted system image.

See Also

- **change** on page 623
- **create** on page 624
- **delete** on page 625
- **next** on page 633

fver

Displays the version of a system image file installed in a specific location on a WX switch.

Syntax — **`fver`** {**`c:`** | **`d:`** | **`e:`** | **`f:`** | **`boot0:`** | **`boot1:`**} [*`filename`*]

- **`c:`** — Nonvolatile storage area containing boot partition 0 (primary).
- **`d:`** — Nonvolatile storage area containing boot partition 1 (secondary).
- **`e:`** — Primary partition of the flash card in the flash card slot.
- **`f:`** — Secondary partition of the flash card in the flash card slot.
- **`boot0:`** — Boot partition 0.
- **`boot1:`** — Boot partition 1.
- *`filename`* — System image filename.

Downloaded from www.Manualslib.com manuals search engine

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — To display the image filenames, use the **dir** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Examples — The following command displays the system image version installed in boot partition 1:

```
boot> fver boot1
File boot1:default version is 3.0.1.
```

See Also

- **dir** on page 627
- **version** on page 636

help

Displays a list of all the boot prompt commands or detailed information for an individual command.

Syntax — **help [***command-name***]**

- *command-name* — Boot prompt command.

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays detailed information for the **fver** command:

```
boot> help fver

        fver  Display the version of the specified device:filename.

  USAGE:  fver [c:file|d:file|e:file|f:file|boot0:file|boot1:file|
boot2:file|boot3:file]

    Command to display the version of the compressed image file
    associated with the given device:filename.
```

See Also

- **ls** on page 632

---

ls

Displays a list of the boot prompt commands.

Syntax — **ls**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — To display help for an individual command, type help followed by the command name (for example, **help boot**).

Downloaded from www.Manualslib.com manuals search engine

Examples — To display a list of the commands available at the boot prompt, type the following command:

```
boot> ls
      ls    Display a list of all commands and descriptions.
    help    Display help information for each command.
autoboot    Display the state of, enable, or disable the autoboot option.
    boot    Load and execute an image using the current boot configuration
profile.
  change    Change the current boot configuration profile.
  create    Create a new boot configuration profile.
  delete    Delete the current boot configuration profile.
    next    Select the next boot configuration profile.
    display    Display the current boot configuration profile.

     dir    Display the contents of the specified boot partition.
    fver    Display the version of the loadable image specified by
device:filename.
 version    Display HW and Bootstrap/Bootloader version information.
   reset    Reset the system.
    test    Display the state of, enable, or disable the tests option.
    diag    Access the diagnostic command CLI.
```

See Also

- **help** on page 631

---

next

Activates and displays the boot profile in the next boot profile slot. (For information about boot profiles, see **display** on page 628.)

Syntax — **`next`**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — A WX switch contains 4 boot profile slots, numbered 0 through 3. This command activates the boot profile in the next slot, in ascending numerical order. If the currently active slot is 3, the command activates the boot profile in slot 0.

Downloaded from www.Manualslib.com manuals search engine

Examples — To activate the boot profile in the next slot and display the profile, type the following command:

```
boot> next

    BOOT Index:    0
    BOOT TYPE:     c
    DEVICE:        boot1:
    FILENAME:      testcfg
    FLAGS:         00000000
    OPTIONS:       run=nos;boot=0
```

See Also

- **change** on page 623
- **create** on page 624
- **delete** on page 625
- **display** on page 628

---

reset

Resets a WX switch's hardware.

Syntax — **reset**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — After resetting the hardware, the **reset** command attempts to load a system image file only if other boot settings are configured to do so.

Examples — To immediately reset the system, type the following command at the boot prompt:

```
boot> reset

WX Bootstrap 3.1 Release
Testing Low Memory 1 ............
Testing Low Memory 2 ............
CISTPL_VERS_1:  4.1   <SanDisk> <SDP> <5/3 0.6>
Reset Cause (0x0100) is WARM
```

Downloaded from www.Manualslib.com manuals search engine

```
3Com WX-4400 Bootstrap/Bootloader

              Version  3.0.2  Release
Compiled on Wed Sep 22 09:18:47 PDT 2004 by

 Bootstrap 0 version:           3.1     Active
Bootloader 0 version:         3.0.2     Active
 Bootstrap 1 version:           3.1
Bootloader 1 version:         3.0.1

    WX-4400 Board Revision:    2.
WX-4400 Controller Revision:    5.
     WXA30001.Rel                 8863722 bytes

BOOT Index:   0
BOOT TYPE:    c
DEVICE:       boot0:
FILENAME:     default
FLAGS:        00000000
OPTIONS:      run=nos;root=md0a
```

See Also

- **boot** on page 621

---

test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether a WX performs a set of self tests prior to the boot process.

Syntax — **`test`** [**`ON`** | **`on`** | **`OFF`** | **`off`**]

- **`ON`** — Enables the poweron test flag.
- **`on`** — Same effect as **ON.**
- **`OFF`** — Disables the poweron test flag.
- **`off`** — Same effect as **OFF**.

Defaults — The poweron test flag is disabled by default.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Downloaded from www.Manualslib.com manuals search engine

Examples — The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

See Also

- **boot** on page 621

version

Displays version information for a WX switch's hardware and boot code.

Syntax — **version**

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the **dir** or **fver** command.

Examples — To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version

3Com WX-4400 Bootstrap/Bootloader

                Version  3.0.2  Release
    Compiled on Wed Sep 22 09:18:47 PDT 2004 by

     Bootstrap 0 version:          3.1     Active
    Bootloader 0 version:        3.0.2     Active
     Bootstrap 1 version:          3.1
    Bootloader 1 version:        3.0.1

       WX-4400 Board Revision:    2.
  WX-4400 Controller Revision:    5.
```

See Also

- **dir** on page 627
- **fver** on page 630

Downloaded from www.Manualslib.com manuals search engine

A OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

Warranty and other service benefits are enabled through product registration. Register your product at **http://eSupport.3com.com/**. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request. If you have trouble registering your product, please contact 3Com Global Services for assistance.

Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services like 3Com Express[SM] and Guardian[SM] can include 24x7 telephone Technical Support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com maintenance and Professional Services is available at **http://www.3com.com/**

Contact your authorized 3Com reseller or 3Com for a complete list of the value-added services available in your area.

Downloaded from www.Manualslib.com manuals search engine

Troubleshoot Online

You will find support tools posted on the 3Com web site at **http://www.3com.com/**

3Com Knowledgebase helps you troubleshoot 3Com products. This query-based interactive tool is located at **http://knowledgebase.3com.com** and contains thousands of technical solutions written by 3Com support engineers.

Access Software Downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at **http://eSupport.3com.com/**

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://eSupport.3com.com/**, or under the Product Support heading at **http://www.3com.com/**

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Telephone Technical Support and Repair

To enable telephone support and other service benefits, you must first register your product at **http://eSupport.3com.com/**

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- Proof of purchase, if you have not pre-registered your product
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Downloaded from www.Manualslib.com manuals search engine

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **http://eSupport.3com.com/**. First time users will need to apply for a user name and password.

Contact Us

3Com offers telephone, e-mail and internet access to Technical Support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below.

Telephone numbers are correct at the time of publication. Find a current directory of contact information posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair			
Australia	1 800 678 515	Philippines	1235 61 266 2602 or
Hong Kong	800 933 486		1800 1 888 9469
India	+61 2 9424 5179 or	P.R. of China	800 810 3033
	000800 650 1111	Singapore	800 6161 463
Indonesia	001 803 61009	S. Korea	080 333 3308
Japan	00531 616 439 or	Taiwan	00801 611 261
	03 3507 5984	Thailand	001 800 611 2000
Malaysia	1800 801 777		
New Zealand	0800 446 398		
Pakistan	+61 2 9937 5083		
You can also obtain support in this region using the following e-mail: **apr_technical_support@3com.com**			
Or request a repair authorization number (RMA) by fax using this number:			+ 65 543 6348
Europe, Middle East, and Africa Telephone Technical Support and Repair			
From anywhere in these regions, call:	+44 (0)1442 435529		

Downloaded from www.Manualslib.com manuals search engine

Country	Telephone Number	Country	Telephone Number
From the following countries, you may use the numbers shown:			
Austria	01 7956 7124	Luxembourg	342 0808128
Belgium	070 700 770	Netherlands	0900 777 7737
Denmark	7010 7289	Norway	815 33 047
Finland	01080 2783	Poland	00800 441 1357
France	0825 809 622	Portugal	707 200 123
Germany	01805 404 747	South Africa	0800 995 014
Hungary	06800 12813	Spain	9 021 60455
Ireland	1407 3387	Sweden	07711 14453
Israel	1800 945 3794	Switzerland	08488 50112
Italy	199 161346	U.K.	0870 909 3266

You can also obtain support in this region using the following URL:
http://emea.3com.com/support/email.html

Latin America **Telephone Technical Support and Repair**

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region using the following:

Spanish speakers, enter the URL:
http://lat.3com.com/lat/support/form.html

Portuguese speakers, enter the URL:
http://lat.3com.com/br/support/form.html

English speakers in Latin America should send e-mail to:
lat_support_anc@3com.com

US and Canada Telephone Technical Support and Repair

1 800 876 3266

Downloaded from www.Manualslib.com manuals search engine

INDEX

A

autoboot 620

B

boot 621

C

change 623
clear {ap | dap} radio 286
clear accounting 203
clear authentication admin 204
clear authentication console 205
clear authentication dot1x 206
clear authentication last-resort 207
clear authentication mac 208
clear authentication proxy 209
clear banner motd 38
clear boot backup- configuration 566
clear boot config 566
clear dap 64
clear dot1x max-req 501
clear dot1x port-control 501
clear dot1x quiet-period 502
clear dot1x reauth-max 503
clear dot1x reauth-period 503
clear dot1x timeout auth-server 504
clear dot1x timeout supplicant 504
clear dot1x tx-period 505
clear fdb 98
clear history 39
clear igmp statistics 422
clear interface 127
clear ip alias 128
clear ip dns domain 129
clear ip dns server 129
clear ip route 130
clear ip telnet 131
clear location policy 210
clear log 609
clear log buffer 609
clear log server 609
clear log trace 590
clear mac-user 211
clear mac-user attr 212
clear mac-user group 212
clear mac-usergroup 213
clear mac-usergroup attr 214
clear mobility-domain 266
clear mobility-domain member 266
clear mobility-profile 215
clear network-domain 274
clear network-domain mode 275
clear network-domain peer 276
clear network-domain seed-ip 277
clear ntp server 131
clear ntp update-interval 132
clear port counters 65
clear port media-type 66
clear port name 66
clear port type 68
clear port-group 65
clear qos 120
clear radio-profile 288
clear radius 486
clear radius client system-ip 487
clear radius server 489
clear rfdetect attack-list 534
clear rfdetect black-list 535
clear rfdetect ignore 535
clear rfdetect ssid-list 536
clear rfdetect vendor-list 537
clear security 12-restrict 99
clear security 12-restrict counters 100
clear security acl 446
clear security acl map 447
clear server group 489
clear server group load-balance 489
clear service-profile 289
clear sessions 519
clear sessions network 521
clear snmp community 133
clear snmp notify profile 133
clear snmp notify target 134
clear snoop 598
clear snoop map 598

Downloaded from www.Manualslib.com manuals search engine

clear spantree portcost 394
clear spantree portpri 395
clear spantree portvlancost 395
clear spantree portvlanpri 396
clear spantree statistics 397
clear summertime 135
clear system 40
clear system countrycode 40
clear system ip-address 40, 136
clear system location 40
clear system name 40
clear timezone 136
clear trace 590
clear user 215
clear user attr 216
clear user group 217
clear usergroup 217
clear usergroup attr 218
clear vlan 101
commit security acl 449
copy 567
create 624
crypto certificate 471
crypto certificate admin 471
crypto certificate eap 471
crypto generate key 473
crypto generate request 474
crypto generate request admin 474
crypto generate request eap 474
crypto generate self-signed 476
crypto generate self-signed admin 476
crypto generate self-signed eap 476
crypto otp 478
crypto otp admin 478
crypto otp eap 478
crypto pkcs12 479
crypto pkcs12 admin 479
crypto pkcs12 eap 479

D

delete 569, 625
dhcp 626
diag 627
dir 570, 627
disable 33
display 628
display {ap | dap} config 290, 391
display {ap | dap} counters 294
display {ap | dap} etherstats 301
display {ap | dap} group 303
display {ap | dap} status 304
display aaa 219
display accounting statistics 222
display arp 137
display auto-tune attributes 309
display auto-tune neighbors 311
display banner motd 41
display base-information 41
display boot 573
display config 574
display crypto ca-certificate 481
display crypto certificate 482
display crypto key ssh 483
display dap connection 313
display dap global 314
display dap unconfigured 316
display dhcp-client 138
display dhcp-server 140
display dot1x 505
display fdb 102
display fdb agingtime 104
display fdb count 105
display igmp 422
display igmp mrouter 426
display igmp querier 427
display igmp receiver-table 429
display igmp statistics 431
display interface 142
display ip alias 143
display ip dns 144
display ip https 145
display ip route 146
display ip telnet 148
display license 42
display load 43
display location policy 224
display log buffer 610
display log config 612
display log trace 613
display mobility-domain config 267
display mobility-domain status 267
display mobility-profile 224
display network-domain 278
display ntp 149
display port counters 69
display port media-type 75
display port poe 71
display port status 73
display port-group 70
display qos 123
display qos dscp-table 124
display radio-profile 317
display rfdetect attack-list 537
display rfdetect black-list 538
display rfdetect clients 539

Downloaded from www.Manualslib.com manuals search engine

display rfdetect countermeasures 541
display rfdetect counters 542
display rfdetect data 544
display rfdetect ignore 546
display rfdetect mobility-domain 546
display rfdetect ssid-list 550
display rfdetect vendor-list 551
display rfdetect visible 552
display roaming station 106
display roaming vlan 108
display security 12-restrict 109
display security acl 450
display security acl editbuffer 450
display security acl hits 451
display security acl info 452
display security acl map 453
display security acl resource-usage 454
display service-profile 321
display sessions 522
display sessions network 525
display snmp community 151
display snmp counters 152
display snmp notify profile 152
display snmp notify target 152
display snmp status 153
display snmp usm 154
display snoop 604
display snoop info 604
display snoop map 605
display snoop stats 606
display spantree 398
display spantree backbonefast 400
display spantree blockedports 401
display spantree portfast 402
display spantree portvlancost 403
display spantree statistics 403
display spantree uplinkfast 409
display summertime 154
display system 43
display timedate 155
display timezone 155
display trace 591
display tunnel 110
display version 576
display vlan config 111

E

et 560

F

fver 630

H

help 46, 631
history 47

L

load config 578
ls 632

M

md5 580
mkdir 580
monitor port counters 76

N

next 633

P

ping 156

Q

quickstart 48
quit 34

R

reset 634
reset {ap | dap} 324
reset port 81
reset system 582
rmdir 584
rollback security acl 458

S

save config 584
save trace 592
set {ap | dap} bias 328
set {ap | dap} blink 330, 332
set {ap | dap} name 333
set {ap | dap} radio antennatype 334
set {ap | dap} radio auto-tune max-power 335
set {ap | dap} radio auto-tune
max-retransmissions 337
set {ap | dap} radio channel 339
set {ap | dap} radio min-client-rate 340
set {ap | dap} radio mode 341
set {ap | dap} radio radio-profile 343

Downloaded from www.Manualslib.com manuals search engine

set {ap | dap} radio tx-power 344
set {ap | dap} upgrade-firmware 346
set accounting {admin | console} 225
set accounting {dot1x | mac | web | last-resort} 227
set arp 158
set arp agingtime 159
set authentication admin 229
set authentication console 231
set authentication dot1x 233
set authentication last-resort 236
set authentication mac 239
set authentication proxy 241
set authentication web 242
set auto-config 48
set banner motd 51
set boot backup- configuration 585
set boot configuration-file 586, 587
set confirm 52
set dap 81
set dap auto 325
set dap auto mode 327
set dap fingerprint 331
set dot1x authcontrol 508
set dot1x key-tx 510
set dot1x max-req 511
set dot1x port-control 512
set dot1x quiet-period 513
set dot1x reauth 513
set dot1x reauth-max 514
set dot1x reauth-period 515
set dot1x timeout auth-server 515
set dot1x timeout supplicant 516
set dot1x tx-period 516
set dot1x wep-rekey 517
set dot1x wep-rekey-period 518
set enablepass 35
set fdb 113
set fdb agingtime 114
set igmp mrsol 436
set igmp mrsol mrsi 436
set igmp qri 440
set igmp querier 441
set igmp receiver 441
set igmp rv 442
set interface 160
set interface dhcp-server 162
set interface status 163
set ip alias 164
set ip dns 164
set ip dns domain 165
set ip dns server 166
set ip https server 167
set ip route 167
set ip snmp server 169
set ip ssh 170
set ip ssh server 171
set ip telnet 171
set ip telnet server 172
set length 53
set license 53
set location policy 244
set log 614
set log buffer 614
set log console 614
set log current 614
set log mark 616
set log server 614
set log sessions 614
set log trace 614
set mac-user 248
set mac-user attr 249
set mac-usergroup attr 254
set mobility profile 255
set mobility-domain member 269
set mobility-domain mode member seed-ip 270
set mobility-domain mode seed domain-name 271
set mobility-profile mode 257
set network-domain mode member seed-ip 280
set network-domain mode seed domain-name 282
set network-domain peer 281
set ntp 173
set ntp server 174
set ntp update-interval 175
set port 83
set port media-type 85
set port name 86
set port negotiation 86
set port poe 87
set port preference 88
set port speed 89
set port trap 90
set port type ap 91
set port type wired-auth 94
set port-group 84
set prompt 54
set qos cos-to-dscp-map 121
set qos dscp-to-cos-map 122
set radio-profile auto-tune channel-config 349
set radio-profile auto-tune channel-holddown 350
set radio-profile auto-tune channel-interval 351
set radio-profile auto-tune power-backoff-timer 352
set radio-profile auto-tune power-config 353
set radio-profile auto-tune power-interval 354
set radio-profile beacon-interval 347, 355
set radio-profile countermeasures 356
set radio-profile dtim-interval 357

Downloaded from www.Manualslib.com manuals search engine

set radio-profile frag-threshold 358
set radio-profile long-retry 359
set radio-profile max-rx-lifetime 360
set radio-profile max-tx-lifetime 361
set radio-profile mode 362
set radio-profile preamble-length 364
set radio-profile rts-threshold 365
set radio-profile service-profile 366
set radio-profile short-retry 369
set radio-profile wmm 370
set radius 490
set radius client system-ip 491
set radius deadtime 490
set radius key 490
set radius retransmit 490
set radius server 494
set radius timeout 490
set refetect ssid-list 560
set rfdetect active-scan 554
set rfdetect attack-list 554
set rfdetect countermeasures 556
set rfdetect countermeasures mac 557
set rfdetect ignore 558
set rfdetect log 559
set rfdetect signature 560
set rfdetect vendor-list 561
set security 12-restrict 114
set security acl 459
set security acl hit-sample-rate 466
set security acl ip icmp 459
set security acl ip ip 459
set security acl ip tcp 459
set security acl ip udp 459
set security acl map 464
set server group 496
set server group load-balance 497
set service-profile auth-dot1x 373
set service-profile auth-fallthru 374
set service-profile auth-psk 375
set service-profile beacon 376
set service-profile cipher-ccmp 377
set service-profile cipher-tkip 378
set service-profile cipher-wep104 379
set service-profile cipher-wep40 380
set service-profile psk-phrase 381
set service-profile psk-raw 382
set service-profile rsn-ie 383
set service-profile shared-key-auth 384
set service-profile ssid-name 384
set service-profile ssid-type 385
set service-profile tkip-mc-time 386
set service-profile web-auth-url 387
set service-profile wep active-multicast-index 388
set service-profile wep active-unicast-index 389
set service-profile wep key-index 390
set service-profile wpa-ie 391
set snmp community 175
set snmp notify profile 177
set snmp notify target 181
set snmp protocol 186
set snmp security 187
set snmp usm 188
set snoop 599
set snoop map 602
set snoop mode 603
set spantree 410
set spantree backbonefast 411
set spantree fwddelay 412
set spantree hello 412
set spantree maxage 413
set spantree portcost 414
set spantree portfast 415
set spantree portpri 416
set spantree portvlancost 417
set spantree portvlanpri 418
set spantree priority 419
set spantree uplinkfast 419
set summertime 191
set system contact 55
set system countrycode 56
set system idle-timeout 58
set system ip-address 59, 192
set system location 59
set system name 60
set timedate 193
set timezone 194
set trace authentication 592
set trace authentication mac-addr 592
set trace authentication port 592
set trace authentication user 592
set trace authorization 593
set trace authorization mac-addr 593
set trace authorization port 593
set trace authorization user 593
set trace dot1x 594
set trace dot1x mac-addr 594
set trace dot1x port 594
set trace dot1x user 594
set trace sm 595
set trace sm mac-addr 595
set trace sm port 595
set trace sm user 595
set user 258
set user attr 259
set user group 260
set user password 258

Downloaded from www.Manualslib.com manuals search engine

set usergroup 261
set usergroup attr 261
set vlan name 116
set vlan port 117
set vlan tunnel-affinity 118
set web-portal 262

T

telnet 195
test 635
traceroute 197

V

version 636

Downloaded from www.Manualslib.com manuals search engine